(19)【発行国】日本国特許庁（ＪＰ）
(12)【公報種別】公開特許公報（Ａ）
(11)【公開番号】特開２００１－２４９８９９（Ｐ２００１－２４９８９９Ａ）
(43)【公開日】平成１３年９月１４日（２００１．９．１４）
(54)【発明の名称】通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体
(51)【国際特許分類第７版】

G06F	15/00	330
		320
	13/00	351
		357
	17/60	176
H04Q	7/38	
H04L	9/32	
	12/66	

【ＦＩ】

G06F	15/00	330 A
		330 Z
		320 A
	13/00	351 Z
		357 A
	17/60	176 A
H04B	7/26	109 R
H04L	9/00	673 B
	11/20	B

【審査請求】未請求
【請求項の数】２６
【出願形態】ＯＬ
【全頁数】８５
(21)【出願番号】特願２０００－６２２１３（Ｐ２０００－６２２１３）
(22)【出願日】平成１２年３月７日（２０００．３．７）
(71)【出願人】
【識別番号】０００００２１８５
【氏名又は名称】ソニー株式会社
【住所又は居所】東京都品川区北品川６丁目７番３５号
(72)【発明者】
【氏名】石橋 義人

【住所又は居所】東京都品川区北品川６丁目７番３５号 ソニー株式会社内
(72)【発明者】
【氏名】浅野 智之
【住所又は居所】東京都品川区北品川６丁目７番３５号 ソニー株式会社内
(72)【発明者】
【氏名】岡 誠
【住所又は居所】東京都品川区北品川６丁目７番３５号 ソニー株式会社内
(74)【代理人】
【識別番号】１００１０１８０１
【弁理士】
【氏名又は名称】山田 英治 （外２名）
【テーマコード（参考）】
5B049
5B085
5B089
5J104
5K030
5K067
9A001
【Ｆターム（参考）】
5B049 AA05 BB00 BB46 CC03 CC22 CC36 CC39 CC48 DD04 EE03 EE05 EE23 EE56 GG04 GG07 GG10
5B085 AE23
5B089 HA01 HA06 HA11 JB14 JB19 KA12 KA17 KB13 KC58 KG03 KH30
5J104 AA07 KA02 KA04 KA05 NA03
5K030 GA15 HA05 HB08 HC01 HC14 HD01 HD06 JT09 LD20
5K067 AA30 BB04 DD17 EE02 EE16 HH11 HH24 HH36
9A001 CC03 CZ05 EE03 JJ01 JJ25 LL03

---

(57)【要約】
【課題】 通信部、暗号処理部を持たない電子機器に対する外部ネットワークを介したメンテナンス、制御を通信の秘密を保持して可能とするサービス提供システムを実現する。
【解決手段】 メンテナンス、制御等の対象である制御対象機器（下位機器）を上位機器にローカルネットワークを介して、あるいはメモリスティック等の情報記録媒体を介してデータ転送可能な構成とする。上位機器は通信手段を有し、サービスセンタから受信したデータをローカルネットワークまたは情報記録媒体を介して制御対象機器（下位機器）に転送する。上位機器はデータを暗号化した上でサービスセンタと通信処理を実行するため、通信データの安全性が保証され、制御情報、あるいは制御情報を提供するために必要となる個人情報などの重要な情報の漏洩が防止される。

【特許請求の範囲】

【請求項１】ローカルネットワークインタフェース手段、または情報記録媒体インタフェース手段の少なくともいずれかを有する制御対象機器と、外部ネットワークに対するインタフェース手段と、該外部ネットワークを使用した転送データの暗号処理を実行する暗号処理手段とを有するとともに、前記制御対象機器のローカルネットワークインタフェース手段または情報記録媒体インタフェース手段のいずれかを介して前記制御対象機器に対してデータ転送可能な構成を有する上位機器とを有し、前記上位機器は、前記外部ネットワークを介して前記制御対象機器に対する制御情報をサービスセンタから受信して、該受信制御情報をローカルネットワークまたは情報記録媒体を介して前記制御対象機器に転送する構成を有することを特徴とする通信手段を介したサービス提供システム。

【請求項２】前記サービスセンタおよび前記上位機器は認証処理手段を有し、前記サービスセンタおよび前記上位機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項３】前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項４】前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間における前記情報記録媒体を介したデータ転送は、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項５】前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理を実行することにより、機器正当性検証処理を実行する構成を有することを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項６】前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理を実行することにより、利用者正当性検証処理を実行する構成を有することを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項７】前記サービスセンタおよび前記上位機器間において送受信されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項８】前記上位機器および前記制御対象機器間において転送されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項９】前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。

【請求項１０】前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。
【請求項１１】前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする請求項１に記載の通信手段を介したサービス提供システム。
【請求項１２】制御対象機器に対する制御情報を通信手段を介して提供するサービス提供方法であり、サービスセンタから、該サービスセンタと通信手段を介して接続される上位機器に対して暗号処理のなされた制御情報を送信するデータ送信ステップと、前記上位機器の受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするサービス提供方法。
【請求項１３】前記サービスセンタから前記上位機器に対するデータ送信ステップの前に、前記サービスセンタと前記上位機器間での認証処理を実行する認証処理ステップを有し、前記データ送信ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１４】前記上位機器から前記制御対象機器に対するデータ転送ステップの前に、前記上位機器と前記制御対象機器間での認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１５】前記上位機器と前記制御対象機器間でのデータ転送が情報記録媒体を介したデータ転送として行われる場合において、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１６】前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理による機器正当性検証処理ステップを実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１７】前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理による利用者正当性検証処理ステップを実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項１８】前記サービスセンタまたは前記上位機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする請求項1-2に記載の通信手段を介したサービス提供方法。
【請求項１９】前記上位機器または前記制御対象機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、前記暗号処理は、生成し

たセッション鍵による暗号化処理として実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２０】前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２１】前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行することを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２２】前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする請求項１２に記載の通信手段を介したサービス提供方法。
【請求項２３】外部ネットワークに対するインタフェース手段と、暗号処理を実行する暗号処理手段と、ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段の少なくともいずれかを有し、前記外部ネットワークを介してサービスセンタから受信した制御対象機器に関する暗号化制御情報を前記ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段を介して制御対象機器に転送する構成を有することを特徴とするサービス仲介装置。
【請求項２４】前記暗号処理手段は前記サービスセンタとの認証処理、前記制御対象機器との認証処理を実行する処理アルゴリズムを格納した構成であることを特徴とする請求項２３に記載のサービス仲介装置。
【請求項２５】前記暗号処理手段は、公開鍵暗号方式、共通鍵暗号方式いずれの処理方式にも対応可能な構成を有することを特徴とする請求項２３に記載のサービス仲介装置。
【請求項２６】制御対象機器に対する制御情報を通信手段を介して提供するサービス提供処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、サービスセンタから通信手段を介して送信される暗号処理のなされた制御情報を受信するデータ受信ステップと、受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするとするプログラム提供媒体。

詳細な説明

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置に関する。さらに詳細には、各種の電子機器、例えばテレビやビデオデッキ、エアコン、冷蔵庫、電子レンジなどの各種電子機器に対して、通信ネットワーク等の通信手段を介して各種の制御を実行したり、メンテナンス等のサービスを提供する構成において、個々の機器を小型で低コストの構成とすることを可能とするとともに、サービス提供時の制御情報、メンテナンス情報、

課金情報等を十分なセキュリティを確保して転送可能とした通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置に関する。

【０００２】

【従来の技術】近年、デジタル技術の発展に伴い、多くの電子機器がマイコン等による制御可能な構成となってきている。また複数のコンピュータを結ぶインターネット等の通信ネットワークにより広い地域をカバーするデジタルネットワークが構築されてきている。電子機器を通信ネットワークに接続することによって、電子機器をネットワークを介して遠隔地から制御したりメンテナンスを行なったり、あるいは電子機器ユーザに対してメンテナンス情報の提供を行なうなど、ネットワークを通じた情報伝達形態が盛んになってきている。

【０００３】具体的には、各種電子機器に対する制御、メンテナンス等のサービスを提供するサービスセンタを設置し、サービスセンタとユーザの電子器間を電話回線、ケーブルテレビ回線、インターネット、無線回線、衛星回線などで接続して各種サービスを提供する構成が実施されている。また、これらのサービス提供システムにおいてユーザ情報、口座情報等の各種決済情報を登録することにより提供したサービスに対して課金処理を行う構成も普及しつつある。

【０００４】

【発明が解決しようとする課題】しかし、このような、電子機器に対するネットワーク等の通信回線を介したサービス提供構成においては、サービス機関とユーザ機器との間をインターネット等の通信手段を介してデータをそのまま送受信することが多いため、例えば個人的な情報が漏洩したり改竄される可能性がある。たとえば、サービス料金に対する課金のためのユーザの銀行口座やクレジットカード番号などの情報は、不正に扱われると重大な被害をもたらす場合があり、インターネットのように複数のユーザが同じ回線を共有するモデルにおいての個人情報を含むデータの送受信は、情報の保護の観点から問題がある。

【０００５】また、現在の通信手段を介したサービス提供システムでは、ネットワーク等を介したサービスを受けるために、サービスを受けるすべての機器がサービスセンタと外部ネットワーク等を経由して直接接続できる構成を持つ必要があった。すなわち、サービス通信手段としてのモデム、インタフェース等がユーザの機器に備わっていることが必要とされている。しかし、このようなサービスを受けるためにすべての機器に通信のためのモジュールを備えることは、コスト面、機器の小型化の点からも好ましいものではない。特に小型化が重要となる機器においてはこの問題は顕著となる。さらに同様の理由で、すべての機器に高度なセキュリティ機能モジュールを構成することも現実的ではなく、これらの問題点がネットワークを介するサービス提供システムの普及を阻む要因の１つとなっている。

【０００６】本発明は、上述の問題点、すなわちサービスを受ける電子機器すべてに通信のためのモジュールを備えることを不要とし、また、機器に高度なセキュリティ機能モジュールを構成する必要性をなくすことを可能としたデータ通信システムおよびデータ通信方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の第１の側面は、ローカルネットワークインタフェース手段、または情報記録媒体インタフェース手段の少なくともいずれかを有する制御対象機器と、外部ネットワークに対するインタフェース手段と、該外部ネットワークを使用した転送データの暗号処理を実行する暗号処理手段とを有するとともに、前記制御対象機器のローカルネットワークインタフェース手段または情報記録媒体インタフェース手段のいずれかを介して前記制御対象機器に対してデータ転送

可能な構成を有する上位機器とを有し、前記上位機器は、前記外部ネットワークを介して前記制御対象機器に対する制御情報をサービスセンタから受信して、該受信制御情報をローカルネットワークまたは情報記録媒体を介して前記制御対象機器に転送する構成を有することを特徴とする通信手段を介したサービス提供システムにある。

【０００８】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器は認証処理手段を有し、前記サービスセンタおよび前記上位機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【０００９】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【００１０】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間における前記情報記録媒体を介したデータ転送は、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【００１１】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理を実行することにより、機器正当性検証処理を実行する構成を有することを特徴とする。

【００１２】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理を実行することにより、利用者正当性検証処理を実行する構成を有することを特徴とする。

【００１３】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器間において送受信されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする。

【００１４】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器間において転送されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする。

【００１５】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供する構成であることを特徴とする。

【００１６】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする。

【００１７】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記

サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする。

【００１８】さらに、本発明の第２の側面は、制御対象機器に対する制御情報を通信手段を介して提供するサービス提供方法であり、サービスセンタから、該サービスセンタと通信手段を介して接続される上位機器に対して暗号処理のなされた制御情報を送信するデータ送信ステップと、前記上位機器の受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするサービス提供方法にある。

【００１９】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタから前記上位機器に対するデータ送信ステップの前に、前記サービスセンタと前記上位機器間での認証処理を実行する認証処理ステップを有し、前記データ送信ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【００２０】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器から前記制御対象機器に対するデータ転送ステップの前に、前記上位機器と前記制御対象機器間での認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【００２１】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器と前記制御対象機器間でのデータ転送が情報記録媒体を介したデータ転送として行われる場合において、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【００２２】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理による機器正当性検証処理ステップを実行することを特徴とする。

【００２３】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理による利用者正当性検証処理ステップを実行することを特徴とする。

【００２４】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタまたは前記上位機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする。

【００２５】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器または前記制御対象機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする。

【００２６】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サー

ビスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供することを特徴とする。

【００２７】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする。

【００２８】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする。

【００２９】さらに、本発明の第３の側面は、外部ネットワークに対するインタフェース手段と、暗号処理を実行する暗号処理手段と、ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段の少なくともいずれかを有し、前記外部ネットワークを介してサービスセンタから受信した制御対象機器に関する暗号化制御情報を前記ローカルネットワークインタフェース手段または情報記録媒体インタフェース手段を介して制御対象機器に転送する構成を有することを特徴とするサービス仲介装置にある。

【００３０】さらに、本発明のサービス仲介装置の一実施態様において、前記暗号処理手段は前記サービスセンタとの認証処理、前記制御対象機器との認証処理を実行する処理アルゴリズムを格納した構成であることを特徴とする。

【００３１】さらに、本発明のサービス仲介装置の一実施態様において、前記暗号処理手段は、公開鍵暗号方式、共通鍵暗号方式いずれの処理方式にも対応可能な構成を有することを特徴とする。

【００３２】さらに、本発明の第４の側面は、制御対象機器に対する制御情報を通信手段を介して提供するサービス提供処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、サービスセンタから通信手段を介して送信される暗号処理のなされた制御情報を受信するデータ受信ステップと、受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするとするプログラム提供媒体にある。

【００３３】本発明の第４の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３４】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３５】

【作用】本発明の機器およびサービスセンタは相互に認証処理を実行し、通信相手の確認を実行する

とともに、送信データの暗号化を行っているため、安全なデータ送受信が可能となる。さらに外部ネットワークに対する通信手段を持たず、サービスセンタに直接接続できない機器も、外部ネットワークと直接接続できる上位機器を介してサービスセンタとの通信を安全に行うことができる。

【００３６】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３７】

【発明の実施の形態】［システム概要］図１は本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置の概要を説明するブロック図である。本発明のシステムはユーザ機器に対するサービスを提供するサービスセンタ１０、サービスセンタ１０とのデータ送受信を実行するサービス仲介装置としての上位機器２０、上位機器２０を経由して、サービスセンタ１０からの制御等を受ける制御対象機器（下位機器）３０、サービスセンタ１０と上位機器２０とを結ぶ電話回線、ＣＡＴＶ回線、衛星、無線、インターネット等の外部ネットワーク通信手段、上位機器２０と制御対象機器（下位機器）３０との間を結ぶ、例えば、ＩＥＥＥ１３９４、ＵＳＢ等の通信インタフェースによって通信可能なローカルネットワークからなる。なお、上位機器２０自体がサービスセンタ１０からの制御、メンテナンス等を受ける制御対象機器となることも可能であり、図１の下側に示す上位機器２０は、この態様を示している。

【００３８】図１に示した各構成要素について説明する。本発明のユーザ側の機器は上位機器２０と制御対象機器（下位機器）３０の２種類に大きく分けられる。以下、各機器およびサービスセンタの構成について説明する。

【００３９】＜上位機器＞サービス仲介装置としての上位機器２０は、サービスセンタ１０と電話回線を介した通信が可能なモデム、あるいは、ＣＡＴＶ回線、衛星、その他の無線回線等を介したデータ送受信が可能な通信手段を有する機器である。また、図１の上部に示すように、制御対象機器（下位機器）３０に対して、サービスセンタ１０からのデータを転送したり、制御対象機器（下位機器）３０からサービスセンタ１０への送信データを転送するための手段を有する。

【００４０】図２に上位機器２０の構成を示す。上位機器２０は、サービスを受ける制御対象機器３０との接続用ローカルネットワークを構成するために用いられるＩＥＥＥ１３９４(アメリカ電気電子学会による接続規格)やＵＳＢ(Universal SerialBus)等のインターフェース部としてのローカルインタフェース２０８を備え、他の機器とのデータ通信が可能である。上位機器２０とサービスセンタ１０との通信は電話回線、ケーブルテレビ回線、無線回線、衛星回線、インターネット接続などによって実行される構成とすればよく、これら各通信方法に従った外部インタフェース２０６を持つ。

【００４１】上位機器２０は暗号化・認証や通信の制御を行う専用のＩＣとしての暗号化通信ＩＣ２０５を備える。この暗号化通信ＩＣ２０５は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。また、ＩＣには上位機器２０固有の識別子（機器ＩＤ）を格納する記憶手段を備えており、機器の認証の際にこのＩＤを利用する。暗号化・認証通信ＩＣ２０５は、外部からＩＤの書き換え等ができないようにＳＡＭ(Secure Application Module) として構成されることが好ましい。

【００４２】暗号化通信ＩＣ２０５内に格納される機器ＩＤはサービスセンタ１０が発行し、サービスセンタのデータベースには発行済みのＩＤが登録される。なお、セキュリティを高めるために機器ＩＤに、例えば検証ビットを付加する等、冗長性を持たせたデータ構成とすることにより、サービスセンタ１０によるサービス実施時に機器ＩＤの検証ビットを用いた検証を実行するような構成として

もよい。このような構成とすることにより、サービスセンタ１０の発行した正規なＩＤ以外の不正なＩＤを持つ機器をサービス対象から排除することが可能となる。

【００４３】公開鍵暗号方式を利用する上で必要となる、上位機器２０自身の公開鍵と秘密鍵の組およびその公開鍵に対応する公開鍵証明書は予め機器の暗号化通信ＩＣ２０５の記憶部に記録されている。公開鍵証明書は信頼できる証明書発行機関、いわゆる認証局（ＣＡ：Certificate Authority）が発行したものである。

【００４４】本発明の通信手段を介したサービス提供システムにおいては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとる。データ転送の際のセキュリティ構成を実現する１つの手法が、転送データの暗号化処理である。

【００４５】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データに戻すことができる。暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、代表的な例としては暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と、暗号化、復号化に異なる鍵を用いる公開鍵暗号方式とがある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。

【００４６】暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の１人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、ディジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな２つの素数（例えば１５０桁）の積を用いるものであり、大きな２つの素数（例えば１５０桁）の積の素因数分解する処理の困難さを利用している。

【００４７】公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Ａが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Ａは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Ａに送付する。利用者Ａは秘密鍵を用いて暗号化文書等を復号する等のシステムである。

【００４８】公開鍵証明書は、公開鍵暗号方式における認証局（ＣＡ：Certificate Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【００４９】公開鍵証明書は、証明書のバージョン番号、認証局（ＩＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【００５０】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵等の全体データに対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【００５１】認証局は、公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）等の処理を行う。

【００５２】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。本発明の図２に示す上位機器２０では、認証局の公開鍵は暗号化通信ＩＣ２０５の内部メモリに格納されている。

【００５３】なお、上位機器の公開鍵、秘密鍵は、サービスセンタ１０に対して機器登録を実行する際に新たに上位機器が生成、あるいはサービスセンタが生成してこれを受信して上位機器に格納する構成としてもよく、この場合、公開鍵証明書が必要であれば、別途認証局から取得する。

【００５４】また、上位機器２０は、複数の鍵の組が格納可能であり、機器が接続するサービスセンタ毎もしくはサービス毎に鍵の組を変更することができる。上位機器２０には、様々な下位機器としての制御対象機器３０がローカル接続可能であり、例えば制御対象機器３０がＡメーカーのテレビであれば、Ａメーカのサービスセンタ接続用の鍵を用い、制御対象機器３０がＢメーカーのエアコンであれば、Ｂメーカのサービスセンタ接続用の鍵を用いる等の構成が可能となる。

【００５５】上位機器２０は、さらに、暗号化通信ＩＣ２０５の処理制御、各インタフェースを介した通信制御、記憶装置２１０のデータアクセス制御等の各種処理を制御するためのＣＰＵ２０１、通信データの一時記憶、処理プログラムの格納部として機能するＲＡＭ、ＲＯＭ等によって構成されるメモリ２０２、機器を操作するユーザに対する指示データ等の表示を行なう表示部２０３、ユーザによる通信開始等の指示を可能とする操作部２０９、ハードディスク、ＣＤ、ＤＶＤ等によって構成される記憶装置２１０を備える。

【００５６】さらに上位機器２０は、機器本来の機能を提供する機器固有部２０４を有する。機器固有部２０４は、機器がたとえばビデオデッキであれば受信データの処理回路や変復調回路、あるいは磁気ドラムやテープ駆動部等であり、例えば電子レンジ等であれば、電子レンジの処理機能を含む。さらに上位機器２０は、メモリースティック、ＦＤ、ＣＤ、ＤＶＤのような情報記録媒体２１１にデータを記録するように構成してもよい。その場合、情報記録媒体２１１とのインターフェース２０７を備える。

【００５７】＜制御対象機器（下位機器）＞制御対象機器（下位機器）３０は、外部ネットワークとの直接接続手段を持たない機器であり、上位機器２０にローカルネットワークを介して接続され、サービスセンタ１０からの制御、メンテナンス等各種サービスを受ける機器である。

【００５８】図３、図４に制御対象機器（下位機器）３０の２つの構成例を示す。図３は、制御対象機器（下位機器）３０が、上位機器と接続するためのローカルネットワークインターフェース３０７を有する構成であり、このローカルネットワークインターフェース３０７を介して上位機器２０と接続され、上位機器２０を介して受領するサービスセンタ１０の制御を受ける。この態様をオンライン型下位機器と呼ぶ。

【００５９】一方、図４に示す制御対象機器（下位機器）３０は、上位機器と接続するためのローカルネットワークインターフェースを持たない構成であり、メモリカード、ＣＤ、ＦＤ等の情報記録媒体３１０に格納された制御情報、メンテナンス情報に基づいて制御を受ける。サービスセンタ１０から受信した制御情報を前述の図２の上位機器の情報記録媒体２１１に格納し、これを制御対象機器

（下位機器）３０に取り付けることによってサービスセンタ１０からの制御をオフライン制御として実行することを可能としたものである。

【００６０】制御対象機器（下位機器）３０の構成について説明する。図３のオンライン型の場合、サービスを受ける制御対象機器（下位機器）３０は、上位機器２０との接続用ローカルネットワークを構成するためＩＥＥＥ１３９４やＵＳＢ(Universal Serial Bus)等のインターフェース部としてのローカルインタフェース３０７を備え、上位機器２０とのデータ通信が可能である。

【００６１】制御対象機器（下位機器）３０は暗号化・認証や通信の制御を行う専用のＩＣとしての暗号化通信ＩＣ３０５を備える。この暗号化通信ＩＣ３０５は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。また、暗号化通信ＩＣ３０５は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。ただし公開鍵暗号方式を利用するためには高い演算能力が必要であることから、資源に制約のある機器においては共通鍵暗号方式のみを利用可能とする構成としてもよい。

【００６２】公開鍵暗号方式を利用する上で必要となる、公開鍵と秘密鍵の組およびその公開鍵に対応する公開鍵証明書は予め制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに記録されている。公開鍵証明書は上述した上位機器２０の場合と同様、信頼できる証明書発行機関、いわゆる認証局（ＣＡ：Certificate Authority）が発行したものである。なお、制御対象機器（下位機器）３０の公開鍵、秘密鍵は、サービスセンタ１０に対して機器登録を実行する際に新たに生成、あるいはサービスセンタが生成してこれを受信して機器に格納する構成としてもよく、この場合、公開鍵証明書が必要であれば、別途認証局から取得する。また、制御対象機器（下位機器）３０は、複数の鍵の組を格納可能とした構成としてもよく、機器が接続するサービスセンタ毎もしくはサービス毎に鍵の組を変更することを可能とした構成としてもよい。なお、サービスセンタ１０の公開鍵は予め機器の暗号化通信ＩＣ３０５の内部メモリに記録されている。なお、共通鍵暗号方式のみを利用する構成とする場合には、共通鍵はサービスセンタ１０によって発行され、制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに格納する。なお、共通鍵は制御対象機器（下位機器）３０の識別子（ＩＤ）に対応してサービスセンタが保持してもよい。

【００６３】制御対象機器（下位機器）３０は、さらに、暗号化通信ＩＣ３０５の処理制御、各インタフェースを介した通信制御、記憶装置３０９のデータアクセス制御等の各種処理を制御するためのＣＰＵ３０１、通信データの一時記憶、処理プログラムの格納部として機能するＲＡＭ、ＲＯＭ等によって構成されるメモリ３０２、機器を操作するユーザに対する指示データ等の表示を行なう表示部３０３、ユーザによる通信開始等の指示を可能とする操作部３０８、ハードディスク、ＣＤ、ＤＶＤ等によって構成される記憶装置３０９を備える。

【００６４】さらに制御対象機器（下位機器）３０は、機器本来の機能を提供する機器固有部３０４を有する。さらに制御対象機器（下位機器）３０は、メモリースティック、ＦＤ、ＣＤ、ＤＶＤのような情報記録媒体３１０にデータを記録するように構成してもよい。その場合、情報記録媒体３１０とのインターフェース３０６を備える。図４のオフライン型の場合、この情報記録媒体３１０を介してサービスセンタ１０からの制御情報を受領する。図３のオンライン型構成では、ローカルネットワークを介するか、あるいは情報記録媒体３１０を介するか、いずれの方法も可能となる。

【００６５】すなわち、図３のオンライン型では、制御対象機器（下位機器）３０はサービスを受ける際、ローカルネットワークインターフェース３０７を用いて上位機器２０に接続し、上位機器２０の外部インタフェース２０６の接続能力を利用してサービスセンタ１０と接続する。このとき通信制

御は制御対象機器（下位機器）３０が独自に行う。また、図４のオフライン型では、上位機器２０が制御対象機器（下位機器）３０の代理としてセンタに接続してデータを送受信し、制御対象機器（下位機器）３０はそのデータを上位機器２０で情報記録媒体に記録し、その情報記録媒体を制御対象機器（下位機器）３０に移動し、制御対象機器（下位機器）３０はその情報記録媒体からデータを読み出す。

【００６６】なお、上述した図３のオンライン型、図４のオフライン型の制御対象機器（下位機器）３０は、暗号化通信ＩＣ３０５を有しており、暗号化処理の可能な構成として説明したが、下位機器においては暗号化を行なわず通信を制御するＩＣだけを備えた構成としてもよく、この場合は通信回線を介してオンライン接続、または記憶媒体を介してオフライン接続した上位機器が通信内容の暗号化処理を代行することが可能である。この場合の制御対象機器（下位機器）３０と上位機器２０との認証には機器識別子（ＩＤ）による認証を実行する。

【００６７】＜サービスセンタ＞サービスセンタ１０の構成例を図５に示す。サービスセンタ１０は、外部ネットワークインタフェース１０５および暗号化通信ＩＣ１０４、サービス提供用データベース１０３、機器情報データベース１０６、利用者情報データベース１０７、ＣＰＵ１０１、メモリ１０２、さらにこれらを接続するデータバスで構成される。

【００６８】暗号化通信ＩＣ１０４は上位機器２０との通信およびデータの暗号化、サービス提供対象機器の認証などの処理を行う。この暗号化通信ＩＣ１０４にはサービスセンタ固有のセンタ識別子（ＩＤ）が記録されており、これは通信相手となる各機器との相互認証の際に利用する。

【００６９】サービスセンタ１０の暗号化通信ＩＣ１０４は公開鍵暗号方式および共通鍵暗号方式を利用するために必要な演算が可能である。機器情報データベース１０６には、通信対象、たまはサービス対象各機器の識別子（ＩＤ）や公開鍵などの情報が格納されている。データ通信において共通鍵暗号方式を利用する機器の場合には、あらかじめ機器ＩＤとそれに対応する共通鍵をこの機器情報データベース１０６に格納しておく。

【００７０】利用者情報データベース１０７には、サービスセンタ１０からのサービスの提供を受ける機器を管理し、サービスの対価等の支払処理を行なうユーザ、すなわちサービス利用者の識別子（ＩＤ）や各利用者の決済情報などが格納されている。サービス提供用データベース１０３には、サービスを提供するために必要なデータが格納されている。ＣＰＵ１０１は、暗号化通信ＩＣ１０４の処理制御、各インタフェースを介した通信制御、各記憶装置のデータアクセス制御等の各種処理を制御を行ない、メモリ１０２は、通信データの一時記憶、処理プログラムの格納部として機能するＲＡＭ、ＲＯＭ等によって構成される。

【００７１】［暗号化・認証レベル］本発明の通信手段を介したサービス提供システムにおいて用いられる公開鍵暗号方式としてはＲＳＡ等、また共通鍵暗号方式としてはＤＥＳ等の暗号方式を用いることが可能であり、必要な強度等を勘案して適切な方式を用いて良い。

【００７２】図６は本発明におけるサービスセンタ１０と上位機器２０、制御対象機器（下位機器）３０との間の接続形態と暗号化・認証レベルをまとめたものである。

【００７３】サービスセンタ１０と上位機器２０とは外部ネットワークで接続されている。また暗号化・認証は公開鍵暗号方式を利用する。上位機器２０と制御対象機器（下位機器）３０との接続の形態には６種類ある。すなわち、（１）制御対象機器（下位機器）３０がローカルネットワークに接続可能で公開鍵暗号方式が利用できる場合、（２）制御対象機器（下位機器）３０がローカルネットワークに接続可能で共通鍵暗号方式のみが利用できる場合、（３）制御対象機器（下位機器）３０がロ

ーカルネットワークに接続可能で暗号が利用できない場合、（４）制御対象機器（下位機器）３０が記録媒体の移動によりデータ交換可能で公開鍵暗号方式が利用できる場合、（５）制御対象機器（下位機器）３０が記録媒体の移動によりデータ交換可能で共通鍵暗号方式のみが利用できる場合、（６）制御対象機器（下位機器）３０が記録媒体の移動によりデータ交換可能で暗号が利用できない場合である。なお、一台の上位機器には複数の下位機器を接続可能であり、上位機器２０は、複数の暗号方式に対応可能な構成とすることにより、様々なタイプの制御対象機器（下位機器）との通信が可能となる。なお、制御対象機器（下位機器）の機器ＩＤを参照することにより、上位機器は配下の下位機器を識別可能である。

【００７４】［全体フロー］本発明の通信手段を介したサービス提供システムにおける上位機器２０および制御対象機器（下位機器）３０のサービスセンタ１０を利用した遠隔サービスの提供処理について、以下説明する。

【００７５】図７から図１０までの図はサービス開始から終了に至るまでの全体の処理の流れを簡潔に示したフロー図である。これらのフロー中に含まれる処理の詳細については、後段で説明する。まず、図７～１０を用いて本発明のサービス提供システムの処理の流れの概要を説明する。

【００７６】まず、図７のフローに示すように、上位機器２０をネットワークを介してサービスセンタ１０に対して初めて接続する場合には、ステップＳ７０１に示すサービスセンタ１０への機器登録を行う。初接続時の処理が終了している場合、もしくは機器登録が不要な処理、例えばフリーメンテナンス提供等の場合には、ステップＳ７０２に示す機器認証のステップに移る。機器認証処理フローを図７に示す。これは上位機器２０およびサービスセンタ１０が相互に通信相手の正当性を確認する手続きである。図に示す機器登録プロトコル、機器認証プロトコルについては後段で詳細に説明する。

【００７７】図７に示す、認証プロトコルを実行することにより、不正な機器がサービスを受けたり、サービスセンタ１０と誤って通信を行うことを防ぐことができる。ステップＳ７０２の機器認証に失敗した場合には、エラー処理を行った後、処理を中止する。機器認証に成功した場合は、必要ならば利用者登録を行う。

【００７８】図８に示す利用者登録手続きでは、サービスセンタ１０の利用者情報データベース（図５に示す１０７）に、機器の利用者情報、例えば氏名、サービス料金決済用のクレジットカード番号、あるいは銀行口座番号等の必要情報を登録（ステップＳ８０１）する。その後パスワード等の利用者認証に必要な情報登録（ステップＳ８０２）も行う。

【００７９】図９は、上段が利用者情報、例えば氏名、クレジット番号等の利用者情報変更手続きを示す処理であり、下段が、パスワード等の利用者認証に必要な情報の変更手続きを示すフローである。利用者情報変更手続きでは最初に利用者認証（ステップＳ９０１）を行う。これは正当な利用者以外の者が不正に他人の利用者情報を変更することを防ぐためである。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いて利用者情報登録（ステップＳ９０２）を行う。

【００８０】利用者情報の登録が完了すると、必要な場合に限り利用者認証に必要な情報、例えばパスワードの利用者認証情報変更手続きを行う。利用者認証情報変更手続きでは、最初に利用者認証を行う。これは正当な利用者以外の者が不正に他人のパスワード等の利用者認証情報を変更することを防ぐためである。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いて利用者認証情報の変更（ステップＳ９０３）を行う。以上の手続きが終了し、サービスを実施する場合にはサービス実施手続きを行う。

【００８１】図１０に制御対象機器の制御、メンテナンス等のサービスの実行処理、すなわちサービス実施手続きフローを示す。サービス実施手続きでは、必要であれば最初に利用者認証を行う。これは正当な利用者以外の者が不正にサービスを受けることを防ぐためである。利用者認証を行うかどうかは、サービスによって異なる。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いてサービスを行う。サービスが完了した後、接続を終了しない場合は機器認証終了時以降の手続きを再度行う。

【００８２】［各プロトコルについて］

（１）機器登録プロトコルａ．上位機器まず、上位機器２０をサービスセンタ１０に対して登録するプロトコルについて説明する。このプロトコルは機器ＩＤ、機種名、機器公開鍵をセンタの機器情報データベースに登録するためのプロトコルである。

【００８３】先の図６で説明したように上位機器２０とサービスセンタ１０との間では、公開鍵暗号方式によって相互認証、データ通信が実行される。公開鍵暗号方式を利用する上で必要となる、上位機器自身の公開鍵と秘密鍵の組があらかじめ上位機器２０の暗号化通信ＩＣ２０５の内部メモリに格納されている場合と、これらの鍵を暗号化通信ＩＣ２０５の内部メモリにあらかじめ格納せず、サービスセンタ１０との接続が必要になった時点でサービスセンタ１０に機器登録を行い、その際にそれぞれの鍵を生成する構成の２つの構成がある。前者の鍵格納済みの場合のプロトコルを図１１に示し、鍵を生成する場合のプロトコルを図１２に示す。

【００８４】図１１、図１２の処理について説明する。機器登録を行う場合、上位機器２０はサービスセンタ１０に機器登録開始要求を送信する。サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを機器に通知する。同時にサービスセンタ１０は自身のセンタ識別子（ＩＤ）を送信する。

【００８５】上位機器２０はサービスセンタ１０から送られてきたサービスセンタ識別子（ＩＤ）によりセンタを確認し、サービスセンタ１０に自身の上位機器識別子（ＩＤ）、機種名および公開鍵証明書を送信する。上位機器２０の暗号化通信ＩＣ２０５にはサービスセンタ１０の公開鍵が格納されており、サービスセンタ１０への送信の際にはこの公開鍵を用いて送信データを暗号化する。

【００８６】なお、図１２に示す例のように、上位機器２０自身が鍵の組を生成する場合には公開鍵証明書のかわりに上位機器２０が生成した公開鍵をセンタに送信する。

【００８７】上位機器２０からサービスセンタ１０への送信データは、サービスセンタ１０の公開鍵で暗号化されているので、送信データに含まれる上位機器識別子（ＩＤ）、機種名等のデータが第三者に漏洩したり、改竄されたりする可能性を排除できる。

【００８８】上位機器識別子（ＩＤ）等のデータを受信したセンタは、サービスセンタ１０自身の秘密鍵で上位機器から送られてきたデータを復号する。復号したデータ中の上位機器識別子（ＩＤ）の検証を行い、正当な識別子（ＩＤ）であれば、送信データ中の上位機器識別子（ＩＤ）、機種名および公開鍵証明書もしくは公開鍵を機器情報データベース１０６に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ１０は上位機器２０に機器登録処理完了通知を返す。データの復号あるいは上位機器識別子（ＩＤ）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラー通知を返す。

【００８９】ｂ．制御対象機器（下位機器）

次に、制御対象機器（下位機器）３０をサービスセンタ１０に対して登録するプロトコルについて説明する。

【００９０】制御対象機器（下位機器）３０が機器登録を行う場合には、オンライン型下位機器とオフライン型下位機器で手順が異なる。さらに公開鍵暗号方式が利用できる機器とできない機器とでも異なる。なお、制御対象機器（下位機器）３０が接続する上位機器２０は、この手続きを行う前に上位機器２０とサービスセンタ１０間での機器認証プロトコルを実施しており、センタとの間で認証がなされているものとする。

【００９１】ｂ－１．公開鍵暗号方式のオンライン型下位機器最初にオンライン型下位機器を用いる場合の手順について図１３に示す。オンライン型下位機器で公開鍵が利用できる場合、公開鍵暗号方式を利用する上で必要となる、制御対象機器（下位機器）３０自身の公開鍵と秘密鍵の組があらかじめ制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに格納されている場合と、これらの鍵を暗号化通信ＩＣ３０５の内部メモリに格納せず、サービスセンタ１０との接続が必要になった時点でサービスセンタ１０に機器登録を行い、その際にそれぞれの鍵を生成する構成の２つの構成がある。前者の鍵格納済みの場合のプロトコルを図１３に示し、鍵を生成する場合のプロトコルを図１４に示す。

【００９２】図１３、図１４の処理について説明する。機器登録を行う場合、最初に制御対象機器（下位機器）３０は上位機器２０に対して機器登録開始要求を発行する。これを受け取った上位機器２０はサービスセンタ１０に機器登録開始要求を中継する。サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを上位機器２０に通知する。そして上位機器２０は機器登録開始が可能であることを制御対象機器（下位機器）３０に対して通知する。

【００９３】この機器登録開始確認通知を受け取ると、制御対象機器（下位機器）３０は制御対象機器（下位機器）自身の機器ＩＤ、機種名、公開鍵証明書をセンタの公開鍵で暗号化し、上位機器に送信する。なお、図１４に示すように下位機器が鍵の組を生成する場合には、公開鍵証明書の代わりに自身の公開鍵を上位機器２０に送信する。これを受け取った上位機器２０は、これらの受信データをそのままサービスセンタに中継する。

【００９４】制御対象機器（下位機器）３０から上位機器２０、サービスセンタ１０へ送信されるデータは、サービスセンタ１０の公開鍵で暗号化されているので、送信データに含まれる制御対象機器（下位機器）識別子（ＩＤ）、機種名等のデータが第三者に漏洩したり、改竄されたりする可能性を排除できる。

【００９５】制御対象機器（下位機器）識別子（ＩＤ）等のデータを受信したセンタは、サービスセンタ１０自身の秘密鍵で上位機器から送られてきたデータを復号する。復号したデータ中の制御対象機器（下位機器）識別子（ＩＤ）の検証を行い、正当な識別子（ＩＤ）であれば、送信データ中の制御対象機器（下位機器）識別子（ＩＤ）、機種名および公開鍵証明書もしくは公開鍵を機器情報データベース１０６に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ１０は上位機器２０に機器登録処理完了通知を返す。データの復号あるいは上位機器識別子（ＩＤ）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラー通知を返す。

【００９６】上位機器２０はサービスセンタ１０から受信した処理完了通知もしくはエラー通知を制御対象機器（下位機器）３０に中継する。

【００９７】ｂ－２．共通鍵暗号方式のオンライン型下位機器公開鍵暗号方式が利用できず、共通鍵方式が利用可能もしくは暗号化機能がないオンライン型下位機器の機器登録手順について述べる。

【００９８】この場合のプロトコルを図１５に示す。この場合も、上位機器２０は機器登録開始が可

能であることを制御対象機器（下位機器）３０に対して通知するまでの処理は同一である。制御対象機器（下位機器）３０が機器登録開始確認通知を受け取ると、制御対象機器（下位機器）３０は自身の機器ＩＤ、機種名を上位機器２０に送信する。

【００９９】この場合、上位機器２０に送信される機器ＩＤ、機種名情報は暗号化されていないが、ローカルネットワーク上であるので外部ネットワークに比べてセキュリティ上の問題は比較的少ないと考えられる。上位機器２０は制御対象機器（下位機器）３０から受け取った情報をサービスセンタ１０の公開鍵で暗号化する。すなわち、上位機器２０がデータの暗号化を代行する。この後の処理は公開鍵暗号方式が利用できる下位機器の場合の手順と同一であるので説明を省略する。

【０１００】ｂ－３．公開鍵暗号方式のオフライン型下位機器続いてオフライン型下位機器における機器登録手順について述べる。オフライン型下位機器で公開鍵暗号方式が利用できる場合、公開鍵暗号方式を利用する上で必要となる、制御対象機器（下位機器）３０自身の公開鍵と秘密鍵の組があらかじめ制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５の内部メモリに格納されている場合と、これらの鍵を暗号化通信ＩＣ３０５の内部メモリに格納せず、サービスセンタ１０との接続が必要になった時点でサービスセンタ１０に機器登録を行い、その際にそれぞれの鍵を生成する構成の２つの構成がある。前者の鍵格納済みの場合のプロトコルを図１６に示し、鍵を生成する場合のプロトコルを図１７に示す。

【０１０１】図１６、図１７の処理について説明する。制御対象機器（下位機器）３０は最初に情報記録媒体を認証する。情報記録媒体３１０は例えばメモリカードであり、メモリカードの識別子等を用いた認証処理が実行される。認証が成立すると、制御対象機器（下位機器）３０は自身の制御対象機器（下位機器）識別子（ＩＤ）、機種名および公開鍵証明書（図１６）もしくは公開鍵（図１７）をサービスセンタの公開鍵で暗号化し、情報記録媒体３１０に転送する。

【０１０２】データ転送が完了した後、情報記録媒体３１０を制御対象機器（下位機器）３０下位機器から取り外し、上位機器２０に装着する。上位機器２０は情報記録媒体２１１（情報記録媒体３１０と同じ）が装着されると、情報記録媒体の認証を開始する。情報記録媒体認証が終了した後、上位機器２０は情報記録媒体からデータを転送（読み出し処理）する。転送終了後、上位機器２０はサービスセンタ１０に機器登録開始要求を制御対象機器（下位機器）３０の代理として行う。

【０１０３】サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを上位機器２０に通知する。そして上位機器２０は情報記録媒体２１１から転送したデータをそのままセンタに送信する。情報記録媒体２１１から読み出された制御対象機器（下位機器）識別子（ＩＤ）等のデータを受信したセンタは、自身の秘密鍵で上位機器２０が中継したデータを復号する。その後復号したデータ中の制御対象機器（下位機器）識別子（ＩＤ）の検証を行い、正当なＩＤであれば、受信した制御対象機器（下位機器）識別子（ＩＤ）、機種名および公開鍵証明書（図１６）もしくは公開鍵（図１７）を機器情報データベース１０６に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ１０は上位機器２０に処理完了通知を返す。データの復号あるいは制御対象機器（下位機器）識別子（ＩＤ）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラー通知を返す。上位機器２０は情報記録媒体２１１に処理完了通知もしくはエラー通知を転送する。その後、情報記録媒体２１１を上位機器２０から制御対象機器（下位機器）３０に移動する。制御対象機器（下位機器）３０は情報記録媒体認証を行った後、サービスセンタ１０からの通知を情報記録媒体から転送する。通知内容がエラー通知であれば、再度機器登録を試みる。

【０１０４】ｂ－４．共通鍵暗号方式のオフライン型下位機器公開鍵暗号方式が利用できず、共通鍵方式が利用可能もしくは暗号化機能がないオフライン型下位機器の機器登録手順について述べる。この場合のプロトコルを図１８に示す。制御対象機器（下位機器）３０は最初に情報記録媒体３１０を認証する。その後、制御対象機器（下位機器）３０は自身の機器ＩＤ、機種名を情報記録媒体３１０に転送する。転送が完了した後、情報記録媒体３１０を制御対象機器（下位機器）３０から取り外し、上位機器２０に装着する。

【０１０５】上位機器２０は情報記録媒体２１１（＝情報記録媒体３１０）が装着されると、情報記録媒体２１１の認証を開始する。情報記録媒体２１１の認証が終了した後、上位機器２０は情報記録媒体２１１からデータを転送する。転送終了後、上位機器２０はサービスセンタ１０に機器登録開始要求を送信する。サービスセンタ１０は要求に応えられる状態であれば、機器登録開始可能であることを上位機器２０に通知する。上位機器２０は情報記録媒体２１１から転送したデータをサービスセンタ１０の公開鍵で暗号化し、センタに送信する。情報記録媒体２１１から読み出された制御対象機器（下位機器）識別子（ＩＤ）等のデータを受信したセンタは、自身の秘密鍵で上位機器２０が中継したデータを復号する。その後復号したデータ中の制御対象機器（下位機器）識別子（ＩＤ）の検証を行い、正当なＩＤであれば、受信した制御対象機器（下位機器）識別子（ＩＤ）、機種名を機器情報データベース１０６に登録する。その後の処理完了通知などの処理は、公開鍵暗号方式が利用できるオフライン型下位機器を用いる場合と同様である。

【０１０６】［機器認証プロトコル］次に、サービスセンタ１０、上位機器２０、制御対象機器（下位機器）３０の相互において実行される機器認証プロトコルの詳細について説明する。機器認証プロトコルは、データ通信を行なう２者間で通信相手の正当性を確認するために実行されるプロセスである。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。以下、上位機器２０を中心として行われる機器認証プロトコルと、制御対象機器（下位機器）３０を中心として行われる機器認証プロトコルについて、それぞれ説明する。

【０１０７】ａ．上位機器まず、上位機器２０とサービスセンタ１０との間で実行される互いの正当性を確認する機器認証プロトコルについて説明する。

【０１０８】図１９にサービスセンタ１０と上位機器２０とが機器認証を行う場合のプロトコルを示す。まず上位機器２０はサービスセンタ１０に機器認証開始要求を送信する。サービスセンタ１０は要求に応えられる状態であれば、機器認証開始可能であることを機器に通知する。この際、サービスセンタ１０は自身のセンタＩＤを送信する。

【０１０９】上位機器２０はサービスセンタ１０から、認証開始可能の応答を受領すると、上位機器２０自身の機器ＩＤを送信する。その後、サービスセンタ１０と上位機器２０との間で相互認証を行う。相互認証の手続きとしては、たとえばＩＳＯ９７９８に示されている手続きを利用することができる。

【０１１０】ＩＳＯ９７９８の相互認証手続きとして、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図２０を用いて説明する。図２０において、公開鍵暗号方式としてＥＣＣを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図２０において、Ａ、Ｂの一方がサービスセンタ１０、他方が上位機器２０に相当する。

【０１１１】まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新た

に６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（Ｘ座標とＹ座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。

【０１１２】公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書認証局（ＣＡ）の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出す。

【０１１３】Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

【０１１４】次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１１５】Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ａｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１１６】両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【０１１７】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１１８】このような相互認証処理において生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行することにより、第三者に対する通信データの漏洩が防止される。なお、データの暗号化に必要なセッション鍵の生成はサービスセンタ１０、上位機器２０のどちらが行ってもよい。相互認証やセッション鍵の交換が失敗した場合には、サービスセンタ１０は上位機器２０にエラーを返す。すべての処理が完了したならば、センタは上位機器に処理完了を通知する。

【０１１９】ｂ－１．オンライン型下位機器次にサービスセンタ１０とオンライン型の制御対象機器（下位機器）３０とが機器認証を行う場合について述べる。この場合のプロトコルを図２１に示す。

【0120】まずオンライン型の制御対象機器（下位機器）３０は上位機器２０に機器認証開始要求を送信する。上位機器２０は要求に応えられる状態であれば、機器認証開始可能であることを制御対象機器（下位機器）３０に通知する。制御対象機器（下位機器）３０は上位機器２０に自身の機器ＩＤを送信する。そして上位機器２０と制御対象機器（下位機器）３０との間で相互認証を行う。

【０１２１】なお、上位機器２０と制御対象機器（下位機器）３０との間での相互認証は、前述のサービスセンタ１０と上位機器２０との間の相互認証処理として説明した図２０の公開鍵暗号方式の認証処理として行なってもよいし、共通鍵暗号方式による相互認証を行なってもよい。

【０１２２】共通鍵暗号方式を用いた相互認証方法を、図２２を用いて説明する。図２２は共通鍵暗号方式としてＤＥＳを用いた例であるが、同様な共通鍵暗号方式であればその他の方法も適用可能である。図２２において、Ａ、Ｂのいずれかが上位機器２０、他方が制御対象機器（下位機器）３０に対応する。

【０１２３】まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。

【０１２４】これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０１２５】次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【０１２６】これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１２７】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１２８】相互認証が成功すれば、上位機器２０はサービスセンタ１０に対して機器認証開始を制御対象機器（下位機器）３０の代理として要求する。サービスセンタ１０は要求に応えられる状態であれば、機器認証開始可能であることを上位機器２０に通知する。上位機器２０はサービスセンタ１０に制御対象機器（下位機器）３０の機器ＩＤを送信する。ここでサービスセンタ１０は下位機器の機器ＩＤの正当性を検証する。正当性の検証は、送付データ中に含まれる機器ＩＤがサービスセンタ１０の持つ機器情報データベース１０６に登録されているか否かをチェックする処理として実行される。機器ＩＤの正当性検証が正常に終了すると、上位機器２０は制御対象機器（下位機器）３０にサービスセンタ１０との直接通信の許可を与える。これ以後、上位機器２０はサービスセンタ１０と制御対象機器（下位機器）３０との間の通信内容には関与しない。

【０１２９】サービスセンタ１０との直接通信許可を受けて、制御対象機器（下位機器）３０はセンタと直接通信して相互認証を行う。相互認証は、例えば前述の図２０、または図２２の例のいずれかを用いて実行される。相互認証が完了すると、以後の相互認証時に生成したセッション鍵（共通鍵）を用いてデータが暗号化されて送受信される。セッション鍵の生成はサービスセンタ１０、制御対象機器（下位機器）３０のどちらが行ってもよい。なお、ここではサービスセンタ１０と上位機器２０

との間および上位機器２０と制御対象機器（下位機器）３０の間でそれぞれ相互認証が完了しているので、サービスセンタ１０と制御対象機器（下位機器）３０との直接の相互認証を省略することも可能である。相互認証やセッション鍵の交換が失敗した場合には、センタは下位機器にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は制御対象機器（下位機器）３０に処理完了を通知する。セッション鍵が制御対象機器（下位機器）３０とサービスセンタ１０の間で共有できれば、オンライン型下位機器は以降で説明する各手続きにおいて上位機器２０と同様に扱うことができる。

【０１３０】なお、暗号化機能を持たない制御対象機器（下位機器）３０の場合には、例えばワンタイムパスワードを用いた認証処理により制御対象機器（下位機器）３０の認証を実行する。この場合、サービスセンタ１０または、上位機器２０がセッション鍵を生成して保持し、外部ネットワークを介するサービスセンタ１０と上位機器２０間のデータ通信をセッション鍵を用いたデータ通信とする。この場合のプロトコルを図２３に示す。

【０１３１】ｂ－２．オフライン型下位機器次に、オフライン型下位機器の機器認証プロトコルについて説明する。この場合のプロトコルを図２４に示す。オフライン型の制御対象機器（下位機器）３０は、先に説明したようにメモリーカード等の情報記録媒体を介して制御情報を受け取る構成である。

【０１３２】オフライン型の制御対象機器（下位機器）３０は、最初に情報記録媒体が下位機器に装着されていなければ装着する。その場合には記録媒体の認証を行なう。この認証処理は、制御対象機器（下位機器）３０と情報記録媒体の構成（暗号処理機能、鍵格納構成）に応じて、前述の対称鍵、非対称鍵、パスワードを用いた方法等により実行される。記録媒体認証が成功すると、制御対象機器（下位機器）３０は機器ＩＤなどの機器認証に必要なデータを情報記録媒体に転送する。転送が終了すると、情報記録媒体を上位機器２０に移動する。

【０１３３】上位機器２０は情報記録媒体がセットされると、情報記録媒体の認証を行った後、媒体から機器認証に必要なデータを転送する。情報記録媒体の認証処理は、制御対象機器（下位機器）３０と情報記録媒体との認証処理と同様前述の対称鍵、非対称鍵、パスワードを用いた方法等により実行される。転送が終了すると上位機器２０と制御対象機器（下位機器）３０との相互認証が情報記録媒体の格納データに基づいて実行される。この間、情報記録媒体の上位機器２０と制御対象機器（下位機器）３０間での移動が必要であれば行う。相互認証が成功すれば、上位機器２０はサービスセンタ１０に機器認証開始を制御対象機器（下位機器）３０に代わって要求する。サービスセンタ１０は要求に応えられる状態であれば、機器認証開始可能であることを上位機器２０に通知する。

【０１３４】次に、上位機器２０はサービスセンタ１０に制御対象機器（下位機器）３０の機器ＩＤを送信する。ここでサービスセンタ１０は制御対象機器（下位機器）３０の機器ＩＤの正当性を検証する。機器ＩＤの正当性検証が正常に終了すれば、制御対象機器（下位機器）３０はサービスセンタ２０と相互認証処理およびセッション鍵の交換を行う。しかし制御対象機器（下位機器）３０とサービスセンタ１０とは直接通信できないため、上位機器２０、および情報記録媒体が介在して行う。この間、必要に応じて情報記録媒体の上位機器２０と制御対象機器（下位機器）３０間での移動が行われる。相互認証が完了すると、以後のデータの暗号化に必要なセッション鍵（共通鍵）を生成する。セッション鍵の生成はサービスセンタ１０、制御対象機器（下位機器）３０のどちらが行ってもよい。なお、暗号化機能を持たない制御対象機器（下位機器）３０の場合には、例えばワンタイムパスワードを用いた認証処理により制御対象機器（下位機器）３０の認証を実行する。この場合、サービスセンタ１０または、上位機器２０がセッション鍵を生成して保持し、外部ネットワークを介するサービスセンタ１０と上位機器２０間のデータ通信をセッション鍵を用いたデータ通信とする。相互認証や

セッション鍵の交換が失敗した場合には、サービスセンタ１０は上位機器２０にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は上位機器２０に処理完了を通知する。上位機器２０は情報記録媒体に処理完了通知もしくはエラー通知を転送する。情報記録媒体が制御対象機器（下位機器）３０に移動されると、制御対象機器（下位機器）３０は情報記録媒体を認証し、記録媒体から処理完了通知もしくはエラー通知を転送（読み出し処理）する。

【０１３５】［利用者登録、情報変更プロトコル］次に、利用者名や決済情報などの利用者情報をサービスセンタ１０の利用者情報データベース１０７（図５参照）に登録するための利用者登録、情報変更プロトコルについて説明する。

【０１３６】ａ．上位機器、オンライン型下位機器まず上位機器２０およびオンライン型の制御対象機器（下位機器）３０の場合の処理について述べる。この場合のプロトコルを図２５に示す。上位機器２０およびオンライン型の制御対象機器（下位機器）３０は、「機器」と総称する。機器はサービスセンタ１０に対して利用者登録の開始要求を行う。サービスセンタ１０は利用者情報登録を行える状態であれば、機器に対して開始確認を通知する。機器は利用者が入力した利用者情報をセッション鍵で暗号化し、機器ＩＤとともに送信する。利用者情報は、氏名や住所、決済情報などである。決済情報は銀行口座、クレジットカード番号、プリペイドカード番号など、有償サービスの決済に必要な情報である。サービスセンタ１０は暗号化された利用者情報を、機器ＩＤに対応したセッション鍵で復号する。

【０１３７】続いてサービスセンタ１０は当該利用者に利用者ＩＤを発行し、その利用者ＩＤおよび利用者情報、機器ＩＤをサービスセンタ１０は内の利用者情報データベース１０７に登録する。データベースへの利用者情報の登録後、サービスセンタ１０は利用者ＩＤをセッション鍵で暗号化し、機器に送信する。機器はこれを受け取ると、暗号化された利用者ＩＤをセッション鍵で復号する。そして利用者ＩＤを利用者に通知する。通知は、制御対象機器（下位機器）３０の例えば表示部３０３（図３参照）において実行される。なお、上位機器において表示することも可能である。ここで利用者が機器を利用するたびに利用者ＩＤを入力する手間を省くために、利用者ＩＤを機器に保存しておき、利用者が自分のＩＤを選択するという方法をとってもよい。最後にサービスセンタ１０は機器に対して、処理完了通知もしくはエラー通知を行う。

【０１３８】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず送受信し、上位機器２０がデータをセッション鍵で暗号化した後、サービスセンタ１０に送信する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、下位機器に送信する。この場合のプロトコルを図２６に示す。

【０１３９】なお、すでにサービスセンタ１０内の利用者情報データベース１０７に利用者情報が登録されており、その情報を変更する場合には、登録手続きの中で利用者ＩＤを発行すること、および利用者ＩＤを上位機器に通知する処理が不要となる。また利用者を特定するための氏名等を入力する代わりに、発行された利用者ＩＤを入力してもよい。この時、サービスセンタ１０は、利用者が利用している機器の機器ＩＤが当該の利用者ＩＤと関連づけられていなければ、利用者情報データベース１０７に機器ＩＤを追加する処理を実行する。その他の部分は利用者情報登録の場合と同一である。この場合のプロトコルを図２７に示す。

【０１４０】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号し

た後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図２８に示す。

【０１４１】ｂ．オフライン型下位機器続いてオフライン型下位機器の場合について述べる。この場合のプロトコルを図２９に示す。記録媒体がオフライン型の制御対象機器（下位機器）３０に装着されていなければ装着する。その場合には記録媒体の認証が必要となる。制御対象機器（下位機器）３０は利用者が入力した利用者情報をセッション鍵で暗号化した後、機器ＩＤとともに情報記録媒体に転送する。転送が完了した後、情報記録媒体を制御対象機器（下位機器）３０から取り外し、上位機器２０に装着する。

【０１４２】上位機器２０は情報記録媒体が装着されると、情報記録媒体の認証を開始する。情報記録媒体の認証が終了した後、上位機器２０は情報記録媒体からデータを転送（読み取り）する。転送終了後、上位機器２０はサービスセンタ１０に利用者登録開始要求を下位機器の代理として行う。サービスセンタ１０は利用者情報登録を行える状態であれば、上位機器２０に対して開始確認を通知する。

【０１４３】上位機器２０は制御対象機器（下位機器）３０からのデータをそのままサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者情報を機器ＩＤに対応したセッション鍵で復号する。続いて当該利用者に利用者ＩＤを発行し、その利用者ＩＤおよび利用者情報、機器ＩＤを利用者情報データベース１０７に登録する。

【０１４４】サービスセンタ１０はデータベースへの利用者情報の登録後、利用者ＩＤを制御対象機器（下位機器）３０とのセッション鍵で暗号化し、上位機器２０に送信する。そしてサービスセンタ１０は上位機器２０に対して、処理完了通知もしくはエラー通知を行う。上位機器２０は、サービスセンタ１０から処理完了通知を受け取ると暗号化された利用者ＩＤを情報記録媒体に転送する。その後、情報記録媒体を上位機器２０から制御対象機器（下位機器）３０に移動する。情報記録媒体が制御対象機器（下位機器）３０に装着されると、制御対象機器（下位機器）３０は情報記録媒体の認証を行う。認証が成功すれば、制御対象機器（下位機器）３０は情報記録媒体内のデータを転送（データ読み取り）する。

【０１４５】次に、制御対象機器（下位機器）３０は情報記録媒体から読み取った暗号化された利用者ＩＤをセッション鍵で復号する。そして利用者ＩＤを利用者に通知する。通知は、制御対象機器（下位機器）３０の例えば表示部３０３（図４参照）において実行される。ここで利用者が機器を利用するたびに利用者ＩＤを入力する手間を省くために、利用者ＩＤを機器に保存しておき、それを利用者が自分のＩＤを選択するという方法をとってもよい。

【０１４６】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３０に示す。

【０１４７】なお、すでにサービスセンタ１０内の利用者情報データベース１０７に利用者情報が登録されており、その情報を変更する場合には、登録手続きの中で利用者ＩＤを発行すること、および利用者ＩＤを上位機器に通知する処理が不要となる。また利用者を特定するための氏名等を入力する代わりに、発行された利用者ＩＤを入力してもよい。この時、サービスセンタ１０は、利用者が利用している機器の機器ＩＤが当該の利用者ＩＤと関連づけられていなければ、利用者情報データベース１０７に機器ＩＤを追加する処理を実行する。その他の部分は利用者情報登録の場合と同一である。この場合のプロトコルを図３１に示す。

【０１４８】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３２に示す。

【０１４９】［利用者認証情報登録プロトコル］利用者を識別するためにはいくつかの方法が考えられるが、ここではパスワードを用いた方法とＩＤカードを用いた場合について説明する。ＩＤカードを用いる場合には、個人別のＩＤを埋め込んだカード、指紋などの生体情報を認識できる機構を備えたカード、あるいは利用者個人の公開鍵・秘密鍵の組を保存しているカードなどを用いることが可能である。ＩＤカードとしては磁気テープを有する接触型カードや、無線通信を行う非接触型カードのどちらを用いてもよい。また、利用者を識別するための利用者認証情報を保存し照合を行う場所としては、機器（上位機器・制御対象機器（下位機器））あるいはサービスセンタが考えられる。機器に保存する場合は機器における利用者の制限などの管理を個別に行うことが容易である。サービスセンタに登録する場合には複数の機器を利用する場合においても、機器ごとに登録作業を行う必要がない。まずパスワード等、認証のための情報を機器もしくはセンタに登録する手続きについて述べる。

【０１５０】ａ．機器に保存利用者のパスワード等の利用者認証情報を機器内部に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する方法である。この場合におけるパスワードの登録について説明する。この場合のプロトコルを図３３に示す。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。

【０１５１】利用者がパスワードを操作部（上位機器の場合、操作部２０９、下位機器の場合操作部３０８）から入力すると、機器は利用者ＩＤと対応するパスワードの組を機器内部のメモリに保存する。この時、パスワードを平文のまま保存するのではなく暗号化を施してもよい。次に、サービスセンタ１０は機器に対して、処理完了もしくはエラーを通知する。

【０１５２】次にＩＤカードを用いる利用者認証情報登録処理について説明する。この場合のプロトコルを図３４に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。機器は利用者ＩＤと対応する利用者認証情報を機器内部のメモリに保存する。次にサービスセンタ１０は機器に対して、処理完了もしくはエラーを通知する。

【０１５３】ｂ．センタに保存（上位機器・オンライン型下位機器）
利用者認証情報をサービスセンタ１０に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する方法である。この場合におけるパスワードの登録について説明する。この場合のプロトコルを図３５に示す。

【０１５４】まず上位機器およびオンライン型の制御対象機器（下位機器）を利用する場合は以下の通りである。機器はサービスセンタ１０に利用者認証情報の登録開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、登録開始可能であることを機器に通知する。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器は利用者ＩＤと対応するパスワードの組をセッション鍵で暗号化し、機器ＩＤとともにサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。続いて、パスワードを利用者情報データベース１０７に登録する。セッション鍵での復号やデータベースへの登録が失敗した場合には、サービスセンタ１０は機器にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は機器に処理完了を通知する。

【０１５５】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３６に示す。
【０１５６】次に、ＩＤカードを用いる方法について説明する。この場合のプロトコルを図３７に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。機器はサービスセンタ１０に利用者認証情報の登録開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、登録開始可能であることを機器に通知する。その後、機器は利用者ＩＤと対応する利用者認証情報の組をセッション鍵で暗号化し、機器ＩＤとともにサービスセンタ１０に送信する。以下の処理はパスワードを用いる場合と同様である。
【０１５７】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図３８に示す。
【０１５８】ｃ．オフライン型下位機器次にオフライン型の制御対象機器（下位機器）の場合の利用者認証情報登録プロトコルについて述べる。まず、この場合におけるパスワードの登録について説明する。この場合のプロトコルを図３９に示す。
【０１５９】オフライン型の制御対象機器（下位機器）３０は利用者に利用者ＩＤおよびパスワードの入力を促す。利用者ＩＤおよびパスワードが入力されると、制御対象機器（下位機器）３０はこれをセッション鍵で暗号化して機器ＩＤとともに情報記録媒体に転送する。情報記録媒体が下位機器から上位機器に移されると、上位機器２０は情報記録媒体の認証を行う。情報記録媒体の認証が成功すれば、上位機器２０は情報記録媒体からデータを転送する。その後、上位機器２０はサービスセンタ１０に利用者認証情報の登録開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、登録開始可能であることを上位機器２０に通知する。上位機器２０は情報記録媒体から転送（読み出し）したデータをそのままセンタに送信する。サービスセンタ１０は暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。続いて、パスワードを利用者情報データベース１０７に登録する。セッション鍵での復号やデータベースへの登録が失敗した場合には、サービスセンタ１０は上位機器２０にエラーを返す。すべての処理が完了したならば、サービスセンタ１０は上位機器２０に処理完了を通知する。サービスセンタ１０から上位機器２０に対するエラー通知、処理完了通知は情報記録媒体を介してオフライン型の制御対象機器（下位機器）３０に転送される。
【０１６０】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４０に示す。
【０１６１】次に、ＩＤカードを用いる利用者認証情報登録プロトコルについて説明する。この場合のプロトコルを図４１に示す。制御対象機器（下位機器）３０は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。以下の処理はパスワードを用いる場合と同様である。
【０１６２】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０

にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４２に示す。

【０１６３】［利用者認証プロトコル］次に、利用者認証情報登録プロトコルで登録した利用者認証情報を用いて、利用者を認証する手続きについて述べる。

【０１６４】ａ．機器に利用者認証情報を保存利用者の利用者認証情報を機器に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する場合の利用者認証の方法について説明する。

【０１６５】利用者認証情報としてパスワードを利用する場合のプロトコルを図４３に示す。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器はメモリに保存されている利用者ＩＤとパスワードの組の中から、利用者ＩＤに対応したパスワードを選び出し、これと入力されたパスワードとを照合する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。照合に失敗した場合はエラー処理を行う。

【０１６６】次にＩＤカードを用いる方法について説明する。この場合のプロトコルを図４４に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。この後、機器は内部のメモリに保存されている利用者ＩＤと利用者認証情報の組の中から、利用者ＩＤに対応した利用者認証情報を選び出し、ＩＤカードから転送した利用者認証情報を照合する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。照合に失敗した場合はエラー処理を行う。

【０１６７】ｂ．センタに利用者認証情報を保存利用者のパスワードをサービスセンタ１０に保存して、サービスの提供等の際に利用者の入力したパスワードと照合する場合の利用者認証の方法について説明する。パスワードを利用する場合のプロトコルを図４５に示す。機器はサービスセンタ１０に利用者認証開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、認証開始可能であることを機器に通知する。機器は利用者が入力した利用者ＩＤを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器は利用者ＩＤと対応するパスワードの組をセッション鍵で暗号化した上で機器ＩＤと共にセンタに送信する。センタは暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。サービスセンタ１０は機器・利用者情報データベース１０７に登録されたパスワードと、機器から送信されたパスワードとを照合する。サービスセンタ１０は照合結果を機器に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベース１０７の当該利用者ＩＤのエントリに送信された機器ＩＤが含まれていない場合には追加する。このことにより利用者が複数の機器を利用する場合にも、利用者ＩＤと機器ＩＤとを関連づけることが可能である。照合に失敗した場合はエラー処理を行う。

【０１６８】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図4-6に示す。

【０１６９】次に、ＩＤカードを用いた利用者認証の方法について説明する。この場合のプロトコルを図４７に示す。機器は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利用者認証情報を転送する。機器はサービスセンタ１０に利用者認証開始を要求する。サービスセンタ１

０は要求に応えられる状態であれば、認証開始可能であることを機器に通知する。機器は利用者ＩＤと対応する利用者認証情報の組をセッション鍵で暗号化した上で機器ＩＤと共にサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者ＩＤと利用者認証情報を機器ＩＤに対応したセッション鍵で復号する。サービスセンタ１０は利用者情報データベース１０７に登録された利用者認証情報と、機器から送信された利用者認証情報とを照合する。さらに、サービスセンタ１０は照合結果を機器に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベース１０７の当該利用者ＩＤのエントリに送信された機器ＩＤが含まれていない場合には追加する。照合に失敗した場合はエラー処理を行う。

【０１７０】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図４８に示す。

【０１７１】ｃ．オフライン型の下位機器の場合次にオフライン型の制御対象機器（下位機器）３０の場合の利用者認証の方法について説明する。パスワードを利用する場合のプロトコルを図４９に示す。オフライン型の制御対象機器（下位機器）３０は利用者に利用者ＩＤおよびパスワードの入力を促す。利用者ＩＤおよびパスワードが入力されれば、制御対象機器（下位機器）３０はこれをセッション鍵で暗号化して機器ＩＤとともに情報記録媒体に転送する。

【０１７２】情報記録媒体が制御対象機器（下位機器）３０から上位機器２０に移されると、上位機器２０は情報記録媒体の認証を行う。情報記録媒体の認証が成功すれば、上位機器２０は情報記録媒体からデータを転送（読み取り）する。そして、上位機器２０はサービスセンタ１０に利用者認証開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、認証開始可能であることを上位機器２０に通知する。通知を受領すると上位機器２０は情報記録媒体から転送したデータをそのままサービスセンタ１０に送信する。サービスセンタ１０は暗号化された利用者ＩＤとパスワードを機器ＩＤに対応したセッション鍵で復号する。サービスセンタ１０は利用者情報データベース１０７に登録された利用者認証情報と、機器から送信された利用者認証情報とを照合する。サービスセンタ１０は照合結果を上位機器２０に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベースの当該利用者ＩＤのエントリに送信された機器ＩＤが含まれていない場合には追加する。照合に失敗した場合はエラー処理を行う。認証結果を受け取った上位機器２０は、情報記録媒体にその結果を転送する。情報記録媒体が上位機器２０から制御対象機器（下位機器）３０に移されると、制御対象機器（下位機器）３０は情報記録媒体の認証を行う。記録媒体認証が成功すれば、下位機器は情報記録媒体からデータを転送（読み取り）する。制御対象機器（下位機器）３０は認証結果を利用者に、例えば表示部３０３を介して通知する。

【０１７３】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に情報記録媒体を介して送信する。この場合のプロトコルを図５０に示す。

【０１７４】次にオフライン型の制御対象機器（下位機器）３０の場合におけるＩＤカードを用いた利用者認証の方法について説明する。この場合のプロトコルを図５１に示す。オフライン型の制御対象機器（下位機器）３０は利用者がＩＤカードをセットすると、ＩＤカードから利用者ＩＤおよび利

用者認証情報を転送する。以下の処理はパスワードを用いる場合と同様である。
【０１７５】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に情報記録媒体を介して送信する。この場合のプロトコルを図５２に示す。
【０１７６】［サービスプロトコル］次に、サービスセンタ１０から上位機器２０を利用した遠隔サービスの提供処理について説明する。
【０１７７】ａ．センター上位機器、センター上位機器－下位機器（オンライン）
まず、サービスセンタ１０と上位機器２０、オンライン型の制御対象機器（下位機器）３０を利用する場合のプロトコルを図５３に示す。ここでは、機器といった場合、上位機器２０と、オンライン型の制御対象機器（下位機器）３０とを含む総称である。
【０１７８】最初に機器はサービスセンタ１０にサービス開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、サービス開始可能であることを機器に通知する。サービスはサービスセンタ１０と機器との間でデータを通信することにより実施される。サービスセンタ１０からサービス提供のためのデータが送信される場合について述べる。
【０１７９】まずサービスセンタのＣＰＵ１０１の制御によりサービス提供用データベース１０３から、例えばメンテナンス情報のようなサービス用データが暗号化通信ＩＣ１０４に送られる。暗号化通信ＩＣ１０４は、そのデータを機器認証の際にサービスセンタと機器との間で交換したセッション鍵により暗号化を施した後、外部ネットワークインタフェース１０５を経由して外部ネットワークに送信する。
【０１８０】上位機器２０側では、暗号化通信ＩＣ２０５が外部ネットワークインタフェース２０８経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じてメモリ２０２やディスク等の記録装置２１０に転送される。ＣＰＵ２０１はメモリ２０２やディスク等の記録装置２１０からデータを読み出して、機器固有部２０４の制御を行う。なお、オンライン型の制御対象機器（下位機器）３０の制御を行なう場合は、上位機器２０と制御対象機器（下位機器）３０間でデータが転送される。
【０１８１】続いてオンライン型の制御対象機器（下位機器）３０からサービスセンタ１０にデータを送信する場合について述べる。まず、オンライン型の制御対象機器（下位機器）３０のＣＰＵ３０１の制御によりデータが暗号化通信ＩＣ３０５に送られる。暗号化通信ＩＣ３０５は、データのセッション鍵による暗号化を施した後、ローカルインタフェース３０７を介して上位機器２０に送信する。上位機器２０は制御対象機器（下位機器）３０からローカルインタフェース２０８を介して受信したデータを外部ネットワークインタフェース２０８を経由して外部ネットワークに送信する。
【０１８２】サービスセンタ１０側では、暗号化通信ＩＣ１０４が外部ネットワークインタフェース１０５経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じて、メモリ１０２やサービス提供用データベース１０３、機器情報データベース１０６、利用者情報データベース１０７に転送される。サービスを提供している間、必要であればサービスセンタ１０のＣＰＵ１０１は課金情報をメモリ１０２もしくは利用者情報データベース１０７に記録する。課金情報とは有償サービスの利用回数や時間、送受信データ量などである。
【０１８３】以上、説明したように、サービスの提供中にサービスセンタ１０と機器との間で行われ

るデータの通信は、セッション鍵を用いて暗号化されているので通信内容の保護が可能となる。サービスの提供が終了すれば、サービスセンタ１０のＣＰＵ１０１は利用者ＩＤを検索キーとして利用者データベースから利用者の決済情報を取得し、決済処理を行う。サービスの提供を終了する際には、終了処理を行う。

【０１８４】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に送信する。この場合のプロトコルを図５４に示す。

【０１８５】２．センター上位機器ー下位機器（オフライン）

次に、オフライン型下位機器に対する遠隔サービスの提供処理について説明する。この場合、サービスはサービスセンタ１０と上位機器２０との間で通信を行い、上位機器２０がオフライン型の制御対象機器（下位機器）３０の代わりにデータを受信して一度保存し、そのデータを情報記録媒体を用いてまとめて下位機器に転送することにより実施される。この場合のプロトコルを図５５に示す。

【０１８６】最初に情報記録媒体が制御対象機器（下位機器）３０に装着されていなければ装着する。その場合には情報記録媒体の認証が必要となる。情報記録媒体の認証が成功すると、制御対象機器（下位機器）３０はサービス名やパラメータなど、サービス開始に必要なデータを媒体に転送する。転送が終了してから、情報記録媒体を上位機器２０に移動する。

【０１８７】上位機器２０は情報記録媒体がセットされると、情報記録媒体認証を行った後、情報記録媒体からサービス開始に必要なデータを転送する。転送が終了すると上位機器２０はサービスセンタ１０にサービス開始を要求する。サービスセンタ１０は要求に応えられる状態であれば、サービス開始可能であることを上位機器２０に通知する。

【０１８８】サービス提供中にデータを上位機器２０と制御対象機器（下位機器）３０との間でやりとりする場合について述べる。上位機器２０が情報記録媒体にデータを転送する場合、記録媒体認証が済んでいなければ、上位機器２０の暗号化通信ＩＣ２０５は情報記録媒体の認証を開始する。情報記録媒体が認証できれば、上位機器２０のＣＰＵ２０１はサービスセンタ１０から制御対象機器（下位機器）３０のために受信したデータを上位機器２０内部の記録装置２１０から読み出し、暗号化通信ＩＣ２０５に転送する。暗号化通信ＩＣ２０５に転送されたデータはそのまま記録媒体インタフェース２０７を経由して情報記録媒体２１１に転送（書き込み）される。

【０１８９】制御対象機器（下位機器）３０が情報記録媒体にデータを転送する場合、記録媒体認証が済んでいなければ、制御対象機器（下位機器）３０の暗号化通信ＩＣ３０５は情報記録媒体の認証を開始する。情報記録媒体が認証できれば、制御対象機器（下位機器）３０のＣＰＵ３０１はメモリ３０２もしくは記録装置３０９からデータを読み出し、暗号化通信ＩＣ３０５に転送する。暗号化通信ＩＣ３０５は転送されたデータをセッション鍵で暗号化し、記録媒体インターフェース３０６経由で情報記録媒体３１０に転送する。

【０１９０】またサービス提供中にデータをサービスセンタ１０と上位機器２０の間でやりとりする場合について述べる。サービスセンタ１０からサービス提供のためのデータが送信される場合について述べる。最初にサービスセンタ１０のＣＰＵ１０１の制御によりサービス提供用データベース１０３からデータが暗号化通信ＩＣ１０４に送られる。暗号化通信ＩＣ１０４は、そのデータを機器認証の際にサービスセンタ１０と制御対象機器（下位機器）３０との間で交換したセッション鍵により暗号化を施した後、外部ネットワークインタフェース１０５を経由して外部ネットワークに送信する。

【０１９１】上位機器２０側では、暗号化通信ＩＣ２０５が外部ネットワークインタフェース２０８経由でデータを受信し、データバスを通じてメモリ２０２やディスク等の記録装置２１０に転送する。
【０１９２】続いて上位機器２０からサービスセンタ１０にデータを送信する場合について述べる。まず、上位機器２０のＣＰＵ２０１の制御により制御対象機器（下位機器）３０とサービスセンタ１０との間で交換されたセッション鍵で暗号化されたデータは、メモリ２０２もしくは記録装置２１０から読み出されて暗号化通信ＩＣ２０５に送られる。暗号化通信ＩＣ２０５はそのデータを外部ネットワークインタフェース２０６を経由して外部ネットワークに送信する。サービスセンタ１０側では、暗号化通信ＩＣ１０４が外部ネットワークインタフェース１０５経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じて、メモリ１０２やサービス提供用データベース１０３、機器情報データベース１０６、利用者情報データベース１０７に転送される。サービスを提供している間、必要であればサービスセンタ１０のＣＰＵ１０１は課金情報をメモリ１０２もしくは利用者情報データベース１０７に記録する。課金情報とは有償サービスの利用回数や時間、送受信データ量などである。
【０１９３】以上のように、サービスの提供中にサービスセンタと機器との間で行われるデータの通信は、セッション鍵を用いて暗号化され通信内容を保護することができる。サービスの提供が終了すれば、サービスセンタ１０のＣＰＵ１０１は利用者ＩＤを検索キーとして利用者データベース１０７から利用者の決済情報を取得し、決済処理を行う。サービスの提供を終了する際には、終了処理を行う。
【０１９４】なお、制御対象機器（下位機器）３０が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器２０がセッション鍵で暗号化した後、サービスセンタ１０にデータ送信を実行する。サービスセンタ１０からのデータは上位機器２０がセッション鍵で復号した後、制御対象機器（下位機器）３０に情報記録媒体を介して送信する。この場合のプロトコルを図５６に示す。
【０１９５】［具体的処理例］以下、本発明の通信手段を介したサービス提供システムおよびサービス提供方法の具体的なサービス提供例について説明する。
【０１９６】＜リモートメンテナンス＞まず、具体的なサービス提供例として、遠隔診断・修復システムについて述べる。この場合のプロトコルを図５７に示す。このシステムは、機器に障害が発生した場合に、障害個所の診断及び修復をサービスセンタ１０からの操作により行う例である。
【０１９７】まず機器の状態を調べるために診断を行う。この診断は、機器のＣＰＵ（上位機器の場合はＣＰＵ２０１、下位機器の場合はＣＰＵ３０１）が機器内部の様々な部分に対して命令を発行してその応答を分析することによっておこなう。診断のためのプログラムは機器内部のメモリやディスク等に予め記録しておく。診断が終了すれば、その結果をサービスセンタ１０に送信する。あるいはセンタの助けを借りて診断を行う構成としてもよい。この場合、機器はサービスセンタ１０に対して診断依頼のメッセージを送信する。診断依頼のメッセージを受け取ったサービスセンタ１０は、該当機器の診断が可能であれば診断命令を発行し、機器に対して送信する。機器はサービスセンタ１０から診断命令を受け取るとその命令を実行し、結果をサービスセンタ１０に送信する。
【０１９８】サービスセンタ１０は機器から送信された結果を分析し、それによって必要ならば再度診断命令を発行し、機器に送信する。サービスセンタ１０が診断が終了したと判断できるまで、上記診断命令の発行から分析の手順を繰り返す。以上のように遠隔診断を行って障害箇所および状態を特定でき、かつ遠隔修復が可能であれば修復の手続きに入る。遠隔修復は診断結果に基づき、サービス

センタ１０が機器の障害を復旧するために必要な修復命令を機器に送信することにより行われる。

【０１９９】サービスセンタ１０のＣＰＵ１０１は診断結果を分析して、修復命令を発行する。この際サービス提供用データベース１０３に蓄積された該当機器あるいは同機種の過去の障害履歴を参照して、最適な命令を選択する。サービスセンタ１０はこの修復命令を機器に送信する。機器は受信した修復命令を機器内のＣＰＵの制御により実行してその結果をセンタに送信する。結果を受信したサービスセンタは、その結果や過去の履歴に基づいて分析を行い、必要ならば再度修復命令を発行し、機器に送信する。必要に応じて利用者へのメッセージを機器の表示部に表示する。そして修復の実行を続けるなどの入力を求める。センタが修復が完了したと判断する、あるいは利用者が修復を終了するまで、上記修復命令の発行から分析の手順を繰り返す。修復を終了する際には、それまでの診断結果および修復内容を機器情報データベース１０６に登録する。データベースに登録された診断結果および修復内容は課金に利用したり、複数の機器のデータをまとめて機器メーカーへフィードバックして機器の改善に役立てたりすることが可能である。そしてセンタは機器に対して遠隔修復の終了を通知する。

【０２００】＜バックアップ・リストア＞本発明の別のサービス提供例として、機器に保存されているデータのバックアップおよびリストア処理をサービスセンタ１０が実行する処理構成について説明する。

【０２０１】これは、機器に保存されている設定情報等のデータをあらかじめサービスセンタ１０の記憶手段にバックアップしておき、データが万一消失してもリストアすることで、その機器を以前の状態のまま利用できるようにするためのものである。最初にバックアップについて説明する。この場合のプロトコルを図５８に示す。

【０２０２】機器はサービスセンタ１０に対してバックアップ開始要求を行う。この要求を受信したサービスセンタ１０は、サービス提供用データベース１０３上にバックアップのための領域の確保を行う。領域確保が成功し、かつバックアップを行える状態にあれば、サービスセンタ１０は機器に対してバックアップ開始確認通知を送信する。開始確認通知を受信した機器は、バックアップ対象のデータをサービスセンタ１０に送信する。サービスセンタ１０は受信したバックアップデータを確保した領域に保存する。保存が終了すると、機器情報データベース１０６にバックアップ日時や保存領域などのバックアップ情報を登録する。そしてサービスセンタ１０は機器に対してバックアップの終了を通知する。

【０２０３】続いてリストアの手順について説明する。この場合のプロトコルを図５９に示す。機器はサービスセンタ１０に対してリストア開始要求を行う。この要求を受信したサービスセンタ１０は、機器ＩＤを検索キーとして機器情報データベース１０６からバックアップ情報を取得する。バックアップ情報の取得に成功し、かつリストアを行える状態にあれば、サービスセンタ１０は機器に対してリストア開始確認通知を送信する。そしてサービスセンタ１０は、バックアップ情報からバックアップデータが保存されているサービス提供用データベース１０３上の領域情報を取り出す。この情報に基づきサービス提供用データベース１０３上の領域からバックアップデータを読み出し、機器に送信する。

【０２０４】機器は受信したバックアップデータをチェックした後、リストアを実行する。リストアが終了すると、機器はサービスセンタ１０に対してリストアの終了を通知する。リストア終了通知を受信したサービスセンタ１０は、機器情報データベース１０６にリストア履歴を登録する。そしてサービスセンタ１０は機器に対してリストアに関する処理の終了を通知する。

【０２０５】＜データ配信（音楽、映像、文字情報など）＞本発明のさらに別のサービス提供例として、データ配信について述べる。

【０２０６】これは、音楽や映像、文字情報などのデータをサービスセンタ１０に蓄積し、利用者の要求に応じてサービスセンタ１０から機器に取り込んで利用できるものである。この場合のプロトコルを図６０に示す。データ配信機能を利用する場合には、まず利用者は機器に設けられた操作部（上位機器の場合は操作部２０９、下位機器の場合は操作部３０８）でデータ配信を開始する操作を行う。利用者からの入力を受け付けた機器はサービスセンタ１０に対してデータ配信開始要求を行う。サービスセンタ１０は、データ配信を行える状態にあれば、機器に対してデータ配信開始確認通知を送信する。開始確認通知を受信した機器は、表示部（上位機器の場合は表示部２０３、下位機器の場合は表示部３０３）にデータ配信開始のメッセージを表示する。さらにサービスセンタ１０は利用可能なデータに関する選択肢を含んだメニューを機器に送信する。機器はこのメニューを受信すると、表示部に出力する。

【０２０７】利用者がメニューの中から必要なデータを選択して操作部に入力すると、機器は選択されたデータが何であるかという情報、たとえばデータ番号をサービスセンタ１０に送信する。サービスセンタ１０は、サービス提供用データベースから必要なデータを取得し、機器に送信する。機器はデータを受信したことを表示部に出力する。そして利用者はデータを再生するなどの操作を行う。利用者が引き続きデータ配信機能を利用する場合には、操作部から必要な入力を行えばよい。データ配信が終了すると、サービスセンタ１０は、必要であれば機器情報データベース１０６にデータ配信履歴を登録する。データベースに登録されたデータ配信履歴は課金に利用したり、複数の機器のデータをまとめて以後提供するデータの検討などのマーケティングに役立てたりすることが可能である。そしてサービスセンタ１０は機器に対してデータ配信の終了を通知する。

【０２０８】＜ヘルプ・チュートリアル＞さらに、本発明の別のサービス提供例として、機器の操作方法を解説するヘルプ機能を提供する例について述べる。これは、機器の操作方法を解説するヘルプデータをサービスセンタ１０に蓄積し、利用者の要求に応じて必要な部分を機器に取り込んで、利用者に提示するものである。この場合のプロトコルを図６１に示す。

【０２０９】このヘルプ機能に関しては、機器にすべてのヘルプデータを保存しておくことも可能であるが、機器には保存のための領域が少ない場合があることや、常に新しいヘルプデータを保持することが困難なことから、全部あるいは一部のヘルプデータをサービスセンタ１０に置く形態とする例である。ヘルプ機能を利用する場合には、まず利用者は操作部（上位機器の場合は操作部２０９、下位機器の場合は操作部３０８）でヘルプを開始する操作を行う。利用者からの入力を受け付けた機器はサービスセンタ１０に対してヘルプ開始要求を行う。ヘルプデータの提供を行える状態にあれば、サービスセンタ１０は機器に対してヘルプ開始確認通知を送信する。

【０２１０】開始確認通知を受信した機器は、ヘルプの必要な部分を指定するデータをサービスセンタ１０に送信する。これを受信したサービスセンタ１０は、サービス提供用データベース１０３から必要なヘルプデータを取得し、機器に送信する。機器は受信したヘルプデータを表示部（上位機器の場合は表示部２０３、下位機器の場合は表示部３０３）に表示する。利用者が引き続きヘルプ機能を利用する場合には、操作部から必要な入力を行えばよい。ヘルプデータの提供が終了すると、機器情報データベースにヘルプ提供履歴を登録する。そしてセンタは機器に対してヘルプの終了を通知する。

【０２１１】また単純なヘルプだけではなく、チュートリアルを提供する、すなわち操作情報を提供

する構成とすることも可能である。これは利用者が機器の利用方法を習得するための機能であり、機器の各部分を操作するとその状況に応じて、表示や操作形態が変化する。この場合のプロトコルを図６２に示す。チュートリアル機能を利用する場合には、まず利用者は操作部でチュートリアルを開始する操作を行う。利用者からの入力を受け付けた機器はセンタに対してチュートリアル開始要求を行う。チュートリアルを行える状態にあれば、センタは機器に対してチュートリアル開始確認通知を送信する。開始確認通知を受信した機器は、表示部にチュートリアル開始のメッセージを表示する。利用者が機器の操作を行うと、機器は操作内容と機器の内部状態をサービスセンタ１０に送信する。サービスセンタ１０はこれらの情報に基づいて、次に提供すべきデータを決定する。そして、サービス提供用データベースから必要なチュートリアルデータを取得し、機器に送信する。

【０２１２】機器は受信したチュートリアルデータを表示部に表示する。利用者が引き続きチュートリアル機能を利用する場合には、操作部から必要な入力を行えばよい。チュートリアルデータの提供が終了すると、機器情報データベースにチュートリアル提供履歴を登録する。そしてセンタは機器に対してチュートリアルの終了を通知する。

【０２１３】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２１４】

【発明の効果】以上説明してきたように、本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体によれば、機器がサービスセンタと直接接続できない構成であった場合でも、通信手段を有する上位機器からローカルネットワークまたは情報記録媒体を介してサービスセンタからの情報を受け取ることが可能となり、制御、メンテナンス等の必要な制御対象機器（下位機器）のすべてに外部ネットワークに接続するための通信インタフェース等の通信手段を構成することが必要とならない。

【０２１５】さらに、本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体によれば、制御、メンテナンス等の必要な制御対象機器（下位機器）が暗号化機能を備えない構成であっても、制御対象機器（下位機器）とローカルネットワークまたは情報記録媒体を介して通信可能な上位機器がデータを暗号化した上でサービスセンタとの通信処理を実行するため、通信データの安全性が保証されていない公衆ネットワークを経由しても、制御情報、あるいは制御情報を提供するために必要となる個人情報などの重要な情報の漏洩が防止可能となる。

(The range of a bibliography + summary + claim)

(19) [Issue country] Japanese Patent Office
(JP) -- (12) [official report classification] public presentation patent journal -- the service offer system which minded (54 [name of invention]) means of communication on (A)
(11) [open number] provisional-publication-of-a-patent 2001-249899 (P2001-249899A) (43) [open day] September 14 (2001. 9.14), Heisei 13 --
The service offer method, service agency equipment, and program offer medium [(51) 7th edition of International Patent Classification] G06F 15/00 330

320

13/00 351

357

17/60 176

H04Q 7/38

H04L 9/32

12/66

[FI] G06F 15/00 330 A

330 Z320A

13/00 351 Z

357 A

17/60 176 A

H04B 7/26 109 R

H04L9/00 673 B

11/20B

[a request for examination] -- un--- claim [number of claims] 26 [application form] OL [number of all pages] 85 (21) [application number] application-for-patent 2000-62213 (P2000-62213) (22) [filing date of application --] -- Heisei 12 -- year 3 month 7 day (2000. 3.7) (71) [applicant] [identification number] 000002185 -- [-- a name -- moreover は名称] Sony Corp. [address or address] 6-7-35, Kitashinagawa, Shinagawa-ku, Tokyo (72) [inventor] [name] stone bridge Yoshito [address or address] 6-7-35, Kitashinagawa, Shinagawa-ku, Tokyo (72) in Sony Corp. [inventor] [name] Asano Tomoyuki [address or address] 6-7-35, Kitashinagawa, Shinagawa-ku, Tokyo (72) in Sony Corp. [inventor] [name] 岡 sincerity [address or address] 6-7-35, Kitashinagawa, Shinagawa-ku, Tokyo (74) in Sony Corp. [representative] [identification number] 100101801 [patent attorney] [name or name] Yamada Eiji (besides two persons) [Theme code (reference)] 5B0495B0855B0895J1045K0305K0679A001 [F term (reference)] 5B049 AA05 BB00 BB46 CC03 CC22 CC36 CC39 CC48 DD04 EE03 EE05 EE23 EE56 GG04 GG07 GG10 5B085 AE23 5B089 HA01 HA06 HA11 JB14 JB19 KA12 KA17 KB13 KC58 KG03 KH30 5J104 AA07 KA02 KA04 KA05 NA03 5K030 GA15 HA05 HB08 HC01 HC14 HD01 HD06 JT09 LD20 5K067 AA30 BB04DD17 EE02 EE16 HH11 HH24 HH36 9A001 CC03CZ05 EE03 JJ01 JJ25 LL03

(57) A [summary] and [subject] The service offer system which holds the secret of communication by the maintenance and control through the external network to an electric device without the communications department and the scrambling section, and is made possible is realized.
[Solution means] The controlled-system apparatus (low rank apparatus) which is objects, such as a maintenance and control, is used as high-order apparatus through information recording media, such as a memory stick, through a local network with the composition in which data transfer is possible.
High-order apparatus has a means of communication, and transmits the data received from the service center to controlled-system apparatus (low rank apparatus) through a local network or an information recording medium.

In order that high-order apparatus may perform a service center and communications processing after enciphering data, the safety of communication data is guaranteed, and disclosure of important information, such as personal information which is needed in order to offer control information or control information, is prevented.

[Claim] Controlled-system apparatus of the [Claim 1] local network interface means or an information recording-medium interface means which has either at least,
While having an interface means against an external network, and a scrambling means to perform scrambling of the transmission data which used this external network
It has high-order apparatus which has the composition in which data transfer is possible to the above-mentioned controlled-system apparatus through either the local network interface means of the above-mentioned controlled-system apparatus, or an information recording-medium interface means.
The above-mentioned high-order apparatus receives the control information over the above-mentioned controlled-system apparatus from a service center through the above-mentioned external network.
The service offer system through the means of communication characterized by having the composition which transmits this reception control information to the above-mentioned controlled-system apparatus through a local network or an information recording medium.
[Claim 2] The above-mentioned service center and the above-mentioned high-order apparatus are the service offer systems which have an attestation processing means and minded [which is characterized by the data transmission and reception between the above-mentioned service center and the above-mentioned high-order apparatus being composition performed only when attestation by attestation processing is materialized] the means of communication of a publication 1.
[Claim 3] The above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus are the service offer systems which have an attestation processing means and minded [which is characterized by the data transmission and reception between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus being composition performed only when attestation by attestation processing is materialized] the means of communication of a publication 1.
[Claim 4] The above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus are the service offer systems minded [Claim / 1 / which is characterized by for the data transfer which has an attestation processing means and minded the above-mentioned information recording medium between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus to be the composition which performs only when attestation by attestation processing of the above-mentioned information

recording medium by the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus is materialized] the means of communication of a publication.
[Claim 5] The above-mentioned service center is the service offer system which minded [which is characterized by to have the composition which performs apparatus justification verification processing] the means of communication of a publication 1 by having the apparatus information data base which registered the apparatus identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and performing collation processing with the apparatus identifier registered into this apparatus information data base, and the apparatus identifier which receives from the above-mentioned high-order apparatus or controlled-system apparatus.
[Claim 6] The above-mentioned service center is the service offer system which minded in a means of communication given in Claim 1 characterized by to have the composition which performs user justification verification processing by having the user information data base which registered the user identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and performing collation processing with the user discernment data registered into this user information data base, and the user discernment data which receive from the above-mentioned high-order apparatus or controlled-system apparatus.
[Claim 7] The data transmitted and received between the above-mentioned service center and the above-mentioned high-order apparatus are the service offer systems which minded [which is characterized by being the data with which encryption processing was made using the effective session key only in the communication session concerned] the means of communication of a publication 1.
[Claim 8] The data transmitted between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus are the service offer systems which minded [which is characterized by being the data with which encryption processing was made using the effective session key only in the communication session concerned] the means of communication of a publication 1.
[Claim 9] The above-mentioned service center is the service offer system minded [Claim / 1 / which is carried out / that it is the composition of offering one service of apparatus diagnostic processing, apparatus restoration processing, data backup processing, data restoration processing, data distribution processing, help data offer processing, and operation information service processing, and / with the feature] the means of communication of a publication to the above-mentioned controlled-system apparatus.
[Claim 10] It is the service offer system which minded [which performs attestation processing between the above-mentioned service center and the above-mentioned high-order apparatus with a public-key crypto system, and is characterized by the attestation processing between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus being composition performed with the system of either a public-key crypto system or a common key encryption system] the means of communication of a publication 1.

[Claim 11] It is the service offer system which minded [which performs data communication between the above-mentioned service center and the above-mentioned high-order apparatus with a common key encryption system, and is characterized by the data communication between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus being composition performed with a common key encryption system] the means of communication of a publication 1.
[Claim 12] It is the service offer method of offering the control information over controlled-system apparatus through a means of communication.
The data transmitting step which transmits the control information for which scrambling was made from the service center to the high-order apparatus connected with this service center through a means of communication,
The data transfer step which transmits the encryption control information which the above-mentioned high-order apparatus received to the above-mentioned controlled-system apparatus through a local network interface or an information recording medium as decode control information decoded in the above-mentioned high-order apparatus as encryption control information,
The service offer method characterized by を有(ing).
[Claim 13] It is the service offer method of having minded [Claim / 12 / which is carried out / performing only when it has the attestation processing step which performs attestation processing between the above-mentioned service center and the above-mentioned high-order apparatus before the data transmitting step to the above-mentioned high-order apparatus from the above-mentioned service center and attestation / in / in the above-mentioned data transmitting step / the above-mentioned attestation processing step / is materialized, and / with the feature] the means of communication of a publication.
[Claim 14] It is the service offer method minded in the means of communication given in Claim 12 characterized by to perform only when it has the attestation processing step which performs attestation processing between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus before the data-transfer step to the above-mentioned controlled-system apparatus from the above-mentioned high-order apparatus and attestation [in / in the above-mentioned data-transfer step / the above-mentioned attestation processing step] is materialized.
[Claim 15] It is the service offer method of having minded [Claim / 12 / carry out performing only when it has / / the attestation processing step which performs attestation processing of the above-mentioned information recording medium by the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus when the data transfer between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus is performed as data transfer through an information recording medium, and attestation / in / in the above-mentioned data-transfer step / the above-mentioned attestation processing step / is materialized with the feature] the means of communication of a publication.

[Claim 16] The above-mentioned service center is the service offer method which minded [which is characterized by to perform the apparatus justification verification processing step by collation processing with the apparatus identifier which has the apparatus information data base which registered the apparatus identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and was registered into this apparatus information data base, and the apparatus identifier which receives from the above-mentioned high-order apparatus or controlled-system apparatus] the means of communication of a publication 12.
[Claim 17] The above-mentioned service center is the service offer method which minded [which is characterized by to perform the user justification verification processing step by collation processing with the user discernment data which have the user information data base which registered the user identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and were registered into this user information data base, and the user discernment data received from the above-mentioned high-order apparatus or controlled-system apparatus] the means of communication of a publication 12.
[Claim 18] It is the service offer method which minded [which is characterized by for either the above-mentioned service center or the above-mentioned high-order apparatus generating an effective session key only in the communication session concerned as a key which enciphers the data transmitted and received mutually, and performing the above-mentioned scrambling as encryption processing with the generated session key] the means of communication of a publication 12.
[Claim 19] It is the service offer method which minded [which is characterized by for either the above-mentioned high-order apparatus or the above-mentioned controlled-system apparatus generating an effective session key only in the communication session concerned as a key which enciphers the data transmitted and received mutually, and performing the above-mentioned scrambling as encryption processing with the generated session key] the means of communication of a publication 12.
[Claim 20] The above-mentioned service center is the service offer method of having minded [Claim / 12 / which is carried out / offering one service of apparatus diagnostic processing, apparatus restoration processing, data backup processing, data restoration processing, data distribution processing, help data offer processing, and operation information service processing, and / with the feature] the means of communication of a publication, to the above-mentioned controlled-system apparatus.
[Claim 21] It is the service offer method which minded [which is characterized by performing attestation processing between the above-mentioned service center and the above-mentioned high-order apparatus with a public-key crypto system, and performing attestation processing between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus with the system of either a public-key crypto system or a common key encryption system] the means of communication of a publication 12.

[Claim 22] It is the service offer method which minded [which performs data communication between the above-mentioned service center and the above-mentioned high-order apparatus with a common key encryption system, and is characterized by the data communication between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus being composition performed with a common key encryption system] the means of communication of a publication 12.
[Claim 23] The service agency equipment characterized by to have the composition which transmits the encryption control information about the controlled-system apparatus of the interface means against an external network, a scrambling means perform scrambling, and a local network interface means or an information recording-medium interface means which has either at least and was received from the service center through the above-mentioned external network to controlled-system apparatus through the above-mentioned local network interface means or an information recording-medium interface means.
[Claim 24] The above-mentioned scrambling means is service agency equipment given in Claim 23 characterized by being the composition of having stored the processing algorithm which performs attestation processing with the above-mentioned service center, and attestation processing with the above-mentioned controlled-system apparatus.
[Claim 25] -- the above-mentioned scrambling means -- a public-key crypto system and a common key encryption system -- service agency equipment given in Claim 23 characterized by having the composition which can respond to any processing system.
[Claim 26] It is the program offer medium which offers the computer program which makes service offer processing in which the control information over controlled-system apparatus is offered through a means of communication perform on computer systems.
The data receiving step which receives the control information for which scrambling to which the above-mentioned computer program is transmitted through a means of communication from a service center was made,
The data transfer step which transmits the received encryption control information to the above-mentioned controlled-system apparatus through a local network interface or an information recording medium as decode control information decoded in the above-mentioned high-order apparatus as encryption control information,
The program offer medium it is supposed that is characterized by を有(ing).

Detailed explanation

[Detailed explanation of invention] [0001] [technical field to which invention belongs] book invention relates to the service offer system through a means of communication, the service offer method, and service agency equipment.
Furthermore, various electric devices, such as various kinds of electric devices, for example, television, a videocassette recorder, an air-conditioner, a refrigerator, and a microwave oven, are received in detail.

While performing various kinds of control or making it possible to be small and to consider each apparatus as the composition of a low cost in the composition which offers service of a maintenance etc. through the means of communication of a communication network etc.

It is related with the service offer system through the means of communication which secured sufficient security and enabled transmission of the control information at the time of service offer, maintenance information, fee collection information, etc., the service offer method, and service agency equipment.

[0002] Many electric devices are becoming controllable composition with a microcomputer etc. with development of a digital technology in recent years [[conventional technical]].

Moreover, the digital network which covers a large area by communication networks, such as the Internet which ties two or more computers, has been built.

By connecting an electric device to a communication network, the communication-of-information form which led the network prospers, such as controlling from a remote place, maintaining, or offering maintenance information for an electric device to an electric device user through a network.

[0003] The service center which offers service of control, a maintenance, etc. to various electric devices is specifically installed, and composition which connects between a user's electronic machines with a service center by a telephone line, a cable TV circuit, the Internet, a radio circuit, satellite connection, etc., and offers various services is carried out.

Moreover, the composition which performs fee collection processing to the service offered by registering various settlement-of-accounts information, such as user information and account information, in these service offer systems is also spreading.

[0004] In the service offer composition through communication lines, such as [Object of the Invention], however such a network to an electric device, since data are transmitted between a service establishment and user machines and received as it is through means of communication, such as the Internet, in many cases, individual information may be revealed or it may be altered.

For example, when information, such as a bank account of the user for the fee collection to courtesy rates and a credit card number, is treated unjustly, serious damage may be brought about and transmission and reception of data including the personal information in the model between which two or more users own the same circuit jointly like the Internet have a problem from a viewpoint of protection of information.

[0005] Moreover, in the service offer system through the present means of communication, in order to receive service through a network etc., all the apparatus that receives service needed to have the composition which makes direct connection via a service center, an external network, etc.

That is, to equip a user's apparatus with the modem as a service means of communication, an interface, etc. is needed.
However, it is not desirable from a cost side and a point of a miniaturization of apparatus to equip all apparatus with the module for communication, in order to receive such service.
In the apparatus it becomes important especially miniaturizing, this problem becomes remarkable.
Furthermore, for the same reason, it is not realistic to constitute an advanced security functional module to all apparatus, either, and it has become one of the factors in which these problems obstruct the spread of the service offer systems through a network.
[0006] This invention aims at offering the data communication system and the data communication method which made it possible to abolish the necessity of making it unnecessary to equip with the module for communication all the above-mentioned problem, i.e., the electric devices which receive service, and constituting an advanced security functional module to apparatus.
[0007] the 1st side of [means for solving subject] book invention
The controlled-system apparatus of a local network interface means or an information recording-medium interface means which has either at least,
While having an interface means against an external network, and a scrambling means to perform scrambling of the transmission data which used this external network
It has high-order apparatus which has the composition in which data transfer is possible to the above-mentioned controlled-system apparatus through either the local network interface means of the above-mentioned controlled-system apparatus, or an information recording-medium interface means.
The above-mentioned high-order apparatus receives the control information over the above-mentioned controlled-system apparatus from a service center through the above-mentioned external network.
It is in the service offer system through the means of communication characterized by having the composition which transmits this reception control information to the above-mentioned controlled-system apparatus through a local network or an information recording medium.
[0008] Further, in one embodiment of the service offer system through the means of communication of this invention, the above-mentioned service center and the above-mentioned high-order apparatus have an attestation processing means, and the data transmission and reception between the above-mentioned service center and the above-mentioned high-order apparatus are characterized by being the composition performed only when attestation by attestation processing is materialized.
[0009] Further, in one embodiment of the service offer system through the means of communication of this invention, the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus have an attestation processing means, and the data

transmission and reception between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus are characterized by being the composition performed only when attestation by attestation processing is materialized.

[0010] In one embodiment of the service offer system through the means of communication of this invention, the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus have an attestation processing means, and the data transfer through the above-mentioned information recording medium between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus carries out that it is the composition of performing with the feature further, only when attestation by attestation processing of the above-mentioned information recording medium by the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus is materialized.

[0011] It carries out that the above-mentioned service center has further the composition which performs apparatus justification verification processing by having the apparatus information data base which registered the apparatus identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and performing collation processing with the apparatus identifier registered into this apparatus information data base, and the apparatus identifier which receives from the above-mentioned high-order apparatus or controlled-system apparatus in one embodiment of the service offer system through the means of communication of this invention with the feature.

[0012] In one embodiment of the service offer system which minded the means of communication of this invention further the above-mentioned service center
The user discernment data which have the user information data base which registered the user identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and were registered into this user information data base,
By performing collation processing with the user discernment data received from the above-mentioned high-order apparatus or controlled-system apparatus, it is characterized by having the composition which performs user justification verification processing.

[0013] In one embodiment of the service offer system through the means of communication of this invention, the data transmitted and received between the above-mentioned service center and the above-mentioned high-order apparatus are further characterized by being the data with which encryption processing was made using the effective session key only in the communication session concerned.

[0014] In one embodiment of the service offer system through the means of communication of this invention, the data transmitted between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus are further characterized by being the data with which encryption processing was made using the effective session key only in the communication session concerned.

[0015] In one embodiment of the service offer system minded in the means of communication of this invention, it carries out that the above-mentioned service center is the

composition of providing one service of apparatus diagnostic processing, apparatus restoration processing, data backup processing, data restoration processing, data distribution processing, help data offer processing, and operation information service processing to the above-mentioned controlled-system apparatus with the feature further.

[0016] Further, in one embodiment of the service offer system through the means of communication of this invention, attestation processing between the above-mentioned service center and the above-mentioned high-order apparatus is performed with a public-key crypto system, and it is characterized by the attestation processing between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus being composition performed with the system of either a public-key crypto system or a common key encryption system.

[0017] Further, in one embodiment of the service offer system through the means of communication of this invention, data communication between the above-mentioned service center and the above-mentioned high-order apparatus is performed with a common key encryption system, and data communication between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus is characterized by being the composition performed with a common key encryption system.

[0018] Further the 2nd side of this invention

It is the service offer method of offering the control information over controlled-system apparatus through a means of communication.

The data transmitting step which transmits the control information for which scrambling was made from the service center to the high-order apparatus connected with this service center through a means of communication,

The data transfer step which transmits the encryption control information which the above-mentioned high-order apparatus received to the above-mentioned controlled-system apparatus through a local network interface or an information recording medium as decode control information decoded in the above-mentioned high-order apparatus as encryption control information,

It is in the service offer method characterized by を有(ing).

[0019] It has the attestation processing step which performs attestation processing between the above-mentioned service center and the above-mentioned high-order apparatus before the data transmitting step to the above-mentioned high-order apparatus from the above-mentioned service center in one embodiment of the service offer method through the means of communication of this invention, and it carries out that the above-mentioned data transmitting step performs only when materialized in the attestation in the above-mentioned attestation processing step with the feature further.

[0020] In one embodiment of the service offer method through the means of communication of this invention, it has further the attestation processing step which performs attestation processing between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus before the data transfer step to the above-mentioned

controlled-system apparatus from the above-mentioned high-order apparatus, and it carries out that the above-mentioned data-transfer step performs only when materialized in the attestation in the above-mentioned attestation processing step with the feature.

[0021] In one embodiment of the service offer method which minded the means of communication of this invention further

[when data transfer between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus is performed as data transfer through an information recording medium]

It has the attestation processing step which performs attestation processing of the above-mentioned information recording medium by the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus, and the above-mentioned data transfer step is characterized by performing, only when the attestation in the above-mentioned attestation processing step is materialized.

[0022] It is characterized by for the above-mentioned service center to perform further the apparatus justification verification processing step by collation processing with the apparatus identifier which has the apparatus information data base which registered the apparatus identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and was registered into this apparatus information data base, and the apparatus identifier which receives from the above-mentioned high-order apparatus or controlled-system apparatus in one embodiment of the service offer method through the means of communication of this invention.

[0023] The above-mentioned service center has the user information data base which registered the user identifier of the above-mentioned high-order apparatus and controlled-system apparatus, and is further characterized by to perform the user justification verification processing step by collation processing with the user discernment data registered into this user information data base, and the user discernment data received from the above-mentioned high-order apparatus or controlled-system apparatus in one embodiment of the service offer method through the means of communication of this invention.

[0024] In one embodiment of the service offer method through the means of communication of this invention, either the above-mentioned service center or the above-mentioned high-order apparatus generates an effective session key only in the communication session concerned further as a key which enciphers the data transmitted and received mutually, and it is characterized by performing the above-mentioned scrambling as encryption processing with the generated session key.

[0025] In one embodiment of the service offer method through the means of communication of this invention, either the above-mentioned high-order apparatus or the above-mentioned controlled-system apparatus generates an effective session key only in the communication session concerned further as a key which enciphers the data transmitted and received

mutually, and it is characterized by performing the above-mentioned scrambling as encryption processing with the generated session key.

[0026] In one embodiment of the service offer method minded in the means of communication of this invention, it carries out that the above-mentioned service center provides one service of apparatus diagnostic processing, apparatus restoration processing, data backup processing, data restoration processing, data distribution processing, help data offer processing, and operation information service processing to the above-mentioned controlled-system apparatus with the feature further.

[0027] Further, in one embodiment of the service offer method through the means of communication of this invention, attestation processing between the above-mentioned service center and the above-mentioned high-order apparatus is performed with a public-key crypto system, and it is characterized by the attestation processing between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus being composition performed with the system of either a public-key crypto system or a common key encryption system.

[0028] Further, in one embodiment of the service offer method through the means of communication of this invention, data communication between the above-mentioned service center and the above-mentioned high-order apparatus is performed with a common key encryption system, and data communication between the above-mentioned high-order apparatus and the above-mentioned controlled-system apparatus is characterized by being the composition performed with a common key encryption system.

[0029] The 3rd side of this invention is further to the service agency equipment characterized by to have the composition which transmits the encryption control information about the controlled-system apparatus of the interface means against an external network, a scrambling means perform scrambling, and a local network interface means or an information recording-medium interface means which has either at least and received from the service center through the above-mentioned external network to controlled-system apparatus through the above-mentioned local network interface means or an information recording-medium interface means.

[0030] In one embodiment of the service agency equipment of this invention, it is further characterized by the above-mentioned scrambling means being the composition of having stored the processing algorithm which performs attestation processing with the above-mentioned service center, and attestation processing with the above-mentioned controlled-system apparatus.

[0031] -- further -- one embodiment of the service agency equipment of this invention -- setting -- the above-mentioned scrambling means -- a public-key crypto system and a common key encryption system --- it is characterized by having the composition which can respond to any processing system.

[0032] Further the 4th side of this invention

It is the program offer medium which offers the computer program which makes service offer processing in which the control information over controlled-system apparatus is offered through a means of communication perform on computer systems.
The data receiving step which receives the control information for which scrambling to which the above-mentioned computer program is transmitted through a means of communication from a service center was made,
The data transfer step which transmits the received encryption control information to the above-mentioned controlled-system apparatus through a local network interface or an information recording medium as decode control information decoded in the above-mentioned high-order apparatus as encryption control information,
It is in the program offer medium it is supposed that is characterized by を有(ing).
[0033] the program offer medium concerning the 4th side of this invention — for example, it is the medium which offers a computer program in form [be / computer / it / readable] to the general purpose computer system which can perform various program codes.
As for a medium, the forms in particular, such as transmission medias, such as storage media, such as CD, and FD, MO, or a network, are not limited.
[0034] Such a program offer medium defines the collaboration-relation on the structure of the computer program and offer medium for realizing the function of a predetermined computer program, or a function on computer system
s.
If it puts in another way, by installing a computer program in computer systems through this offer medium, on computer systems, a collaboration-action is demonstrated and the same action effect as other sides of this invention can be acquired. [0035] Since the apparatus and the service center of [action] book invention are enciphering transmitting data while they perform attestation processing mutually and perform a check of a communication partner, the safe data transmission and reception of them are attained. Furthermore, it cannot have a means of communication for an external network, but the apparatus which does not make direct connection can also perform communication with a service center to a service center safely through an external network and the high-order apparatus which makes direct connection.
[0036] The purpose, the feature, and advantage of further others of this invention will become clear [rather than] by detailed explanation based on the case of the operation and the drawing to attach of this invention mentioned later.
[0037] [Form of implementation of invention] [system outline] figure 1 is the service offer system through the means of communication of this invention, the service offer method, and a block diagram explaining the outline of service agency equipment.
The system of this invention goes via the high-order apparatus 20 as service agency equipment which performs data transmission and reception with the service center 10 and service center 10 which offer the service to a user machine, and high-order apparatus 20.

The telephone line which ties the controlled-system apparatus (low rank apparatus) 30 which receives the control from a service center 10 etc., and a service center 10 and high-order apparatus 20,
Between external network means of communication, such as a CATV circuit, a satellite, radio, and the Internet, high-order apparatus 20, and controlled-system apparatus (low rank apparatus) 30 is connected, for example, it consists of a local network which can communicate with communication interfaces, such as IEEE1394 and USB.
In addition, it is also possible to become controlled-system apparatus by which high-order apparatus 20 the very thing receives the control from a service center 10, a maintenance, etc., and the high-order apparatus 20 shown in Fig. 1 bottom shows this mode.
[0038] Explain each component shown in Fig. 1.
As for the apparatus of the users of this invention, high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30 are roughly divided into two kinds. Hereafter, the composition of each apparatus and a service center is explained.
[0039] The high-order apparatus 20 as <high-order apparatus> service agency equipment is apparatus which has the means of communication in which the data transmission and reception through the modem in which communication through a service center 10 and a telephone line is possible or a CATV circuit, a satellite, other radio circuits, etc. are possible.
Moreover, as shown in the upper part of Fig. 1, it has a means for transmitting the data from a service center 10, or transmitting the transmitting data from controlled-system apparatus (low rank apparatus) 30 to a service center 10 to controlled-system apparatus (low rank apparatus) 30.
[0040] The composition of high-order apparatus 20 is shown in Fig. 2.
High-order apparatus 20 is equipped with the local interface 208 as the interface sections, such as IEEE1394 (connection standard by U.S. Institute of Electrical and Electronic Engineers), and USB (Universal SerialBus), used since the local network for connection with the controlled-system apparatus 30 which receives service is constituted, and data communication with other apparatus is possible for it.
The communication with high-order apparatus 20 and a service center 10 has the composition, then the external interface 206 which was good and followed each [these] correspondence procedure performed by a telephone line, the cable TV circuit, a radio circuit, satellite connection, an Internet connectivity, etc.
[0041] High-order apparatus 20 is equipped with the encryption communication IC 205 as IC of the exclusive use which performs control of encryption and attestation, or communication.
Operation required in order to use a public-key-crypto system and a common key encryption system is possible for this encryption communication IC 205.

Moreover, IC is equipped with a memory means to store an identifier (apparatus ID) peculiar to high-order apparatus 20, and this ID is used in the case of attestation of apparatus.
As for encryption / attestation communication IC 205, it is desirable to be constituted as SAM (Secure Application Module) so that rewriting of ID etc. cannot be performed from the exterior.
[0042] A service center 10 publishes the apparatus ID stored in the encryption communication IC 205, and published ID is registered into the data base of a service center.
In addition, in order to raise security, it is good also as composition which performs verification which used the verification bit of Apparatus ID at the time of the service implementation by a service center 10 by considering it as the data composition which gave redundancy, such as adding for example, a verification bit, to Apparatus ID.
By considering it as such composition, it becomes possible to eliminate for service apparatus with inaccurate ID other than regular ID which the service center 10 published.
[0043] The public key certificate corresponding to the group of the public key and secret key of high-order apparatus 20 self which are needed when using a public-key crypto system, and its public key is beforehand recorded on the memory section of the encryption communication IC 205 of apparatus.
The certificate issue organization which can trust it, and the so-called certificate authority (CA:Certificate Authority) publish a public key certificate.
[0044] Take the data transfer composition which transmits required information, namely, took security into consideration after checking that a data sending end and the data reception side were the regular candidates for data transceiver mutually in the service offer system through the means of communication of this invention.
One technique of realizing security composition in the case of data transfer is encryption processing of transmission data.
[0045] Encryption data can be returned to the decode data which can be used by decryption processing in a predetermined procedure.
There are the so-called various common key encryptosystem-ized systems using a key common to encryption and decryption as a typical example although seeds are, and a public-key crypto system using a key which is different in encryption and decryption in the mode of the data encryption and the decryption method using an encryption key and a decryption key.
A public-key crypto system is taken as the secret key which keeps one key as what is different in the key of an addresser and a receiving person, and keeps another side secret as a public key which an unspecified user can use.
For example, use a data encryption key as a public key, and let a decode key be a secret key.

[0046] Since one specific person should just have the secret key which has the necessity of keeping it secret in a public-key crypto system unlike the so-called common key encryption system using a key common to encryption and decryption, it is advantageous in management of a key.
However, many public-key crypto systems for an object with few [as compared with a common key encryptosystem-ized system, a processing data rate is slow, and] amounts of data, such as delivery of a secret key and a digital signature, are used.
A RSA (Rivest-Shamir-Adleman) code is one of the typical things of a public-key crypto system.
This uses the product of two very big prime numbers (for example, 150 figures), and uses the difficulty of the processing of the product of two big prime numbers (for example, 150 figures) which carries out factorization into prime factors.
[0047] In the public-key crypto system, many methods of using the certificate proving whether the public key which is the composition whose use is enabled and distributes a public key to many and unspecified persons is just, and the so-called public key certificate are used.
For example, User A generates the pair of a public key and a secret key, sends the generated public key to a certificate authority, and a public key certificate comes to hand from a certificate authority.
Generally User A exhibits a public key certificate.
An unspecified user receives a public key through a predetermined procedure from a public key certificate, enciphers a document etc., and sends to User A.
User A is the system of decoding an encryption document etc. using a secret key.
[0048] A public key certificate is a certificate which the certificate authority (CA:Certificate Authority) in a public-key crypto system publishes, and when a user submits self ID, a public key, etc. to a certificate authority, it is a certificate which the certificate authority side adds information, such as ID of a certificate authority, and the term of validity, adds the signature by a certificate authority further, and is drawn up.
[0049] A public key certificate includes public key and electronic signature of the algorithm used for the version number of a certificate, the consecutive numbers of the certificate which a certificate authority (IA) assigns to a certificate user, and electronic signature and a parameter, the name of a certificate authority, the term of validity of a certificate, a certificate user's name (user ID), and a certificate user.
[0050] Electronic signature is the data which generated the hash value with the application of the Hash Function to the whole public key data of the name of the algorithm used for the version number of a certificate, the consecutive numbers of the certificate which a certificate authority assigns to a certificate user, and electronic signature and a parameter, the name of a certificate authority, the term of validity of a certificate,

and a certificate user, and a certificate user, and were generated using the secret key of a certificate authority to the hash value.
[0051] a certificate authority updates the public key certificate with which the term of validity went out, and processes creation of the inaccurate person list of [for excluding the user who performed injustice], management, distribution (this -- リボケーション: -- referred to as Revocation), etc. while it publishes a public key certificate.
[0052] On the other hand, in case this public key certificate is used, using the public key of the certificate authority which self holds, a user verifies the electronic signature of the public key certificate concerned, after he succeeds in verification of electronic signature, he picks out a public key from a public key certificate, and uses the public key concerned.
Therefore, all the users using a public key certificate need to hold the public key of a common certificate authority.
The public key of a certificate authority is stored in the internal memory of the encryption communication IC 205 by the high-order apparatus 20 shown in Fig. 2 of this invention.
[0053] In addition, in case the public key of high-order apparatus and a secret key perform apparatus registration to a service center 10, its high-order apparatus is newly good also as generation or composition which a service center generates, receives this and is stored in high-order apparatus, and in this case, if the public key certificate is required, they will be separately acquired from a certificate authority.
[0054] Moreover, high-order apparatus 20 can store the group of two or more keys, and can change the group of a key for every service center which apparatus connects, and every service.
Local connection of the controlled-system apparatus 30 as various low rank apparatus is possible, for example, if controlled-system apparatus 30 is A maker's television, the composition of using the key for service center connection of B maker using the key for service center connection of A maker, if controlled-system apparatus 30 is B maker's air-conditioner is attained at high-order apparatus 20.
Further high-order apparatus 20 [0055] Processing control of the encryption communication IC 205,
CPU201 for controlling various processings through each interface, such as communication control and data access control of storage 210, the temporary storage of communication data,
The control unit 209 which enables directions of the communication start by the display section 203 and the user who display the directions data to the memory 202 constituted by RAM which functions as the storing section of a processing program, ROM, etc., and the user who operates apparatus etc., a hard disk, CD,
It has the storage 210 constituted with DVD etc.

[0056] High-order apparatus 20 has further the apparatus peculiar section 204 which offers the function of apparatus original.
If the apparatus peculiar section 204 is a processing circuit, a strange recovery circuit or a magnetic drum, the tape drive section, etc. of receiving data if apparatus is a videocassette recorder, for example, it is a microwave oven etc., it includes the processing function of a microwave oven.
Furthermore, you may constitute high-order apparatus 20 so that data may be recorded on a memory stick and an information recording medium 211 like FD, CD, and DVD.
In that case, it has the interface 207 with the information recording medium 211.
[0057] <Controlled-system apparatus (low rank apparatus)> controlled-system apparatus (low rank apparatus) 30 is apparatus without a direct connection means with an external network, and is apparatus which is connected to high-order apparatus 20 through a local network, and receives various services, such as control from a service center 10, and a maintenance.
[0058] Two examples of composition of controlled-system apparatus (low rank apparatus) 30 are shown in Fig. 3 and Fig. 4.
Controlled-system apparatus (low rank apparatus) 30 is the composition of having the local network interface 307 for connecting with high-order apparatus, and is connected with high-order apparatus 20 through this local network interface 307, and Fig. 3 receives control of the service center 10 received through high-order apparatus 20.
This mode is called online type low rank apparatus.
[0059] On the other hand, the controlled-system apparatus (low rank apparatus) 30 shown in Fig. 4 is composition without the local network interface for connecting with high-order apparatus, and receives control based on the control information and maintenance information which were stored in the information recording media 310, such as a memory card, and CD, FD.
The control information received from the service center 10 is stored in the information recording medium 211 of the high-order apparatus of the above-mentioned figure 2, and it makes it possible to perform control from a service center 10 as off-line control by attaching this in controlled-system apparatus (low rank apparatus) 30.
[0060] Explain the composition of controlled-system apparatus (low rank apparatus) 30.
In the online type case of Fig. 3, since the controlled-system apparatus (low rank apparatus) 30 which receives service constitutes the local network for connection with high-order apparatus 20, it is equipped with the local interface 307 as the interface sections, such as IEEE1394 and USB (Universal Serial Bus), and data communication with high-order apparatus 20 is possible for it.
[0061] Controlled-system apparatus (low rank apparatus) 30 is equipped with the encryption communication IC 305 as IC of the exclusive use which performs control of encryption and attestation, or communication.

Operation required in order to use a public-key crypto system and a common key encryption system is possible for this encryption communication IC 305.
Moreover, operation required in order to use a public-key crypto system and a common key encryption system is possible for the encryption communication IC 305.
However, since high operation capability is required in order to use a public-key crypto system, it is good also as composition which enables use only of a common key encryption system in the apparatus which has restrictions in resources.
[0062] The public key certificate corresponding to the group of the public key and secret key which are needed when using a public-key crypto system, and its public key is beforehand recorded on the internal memory of the encryption communication IC 305 of controlled-system apparatus (low rank apparatus) 30.
The certificate issue organization which can trust it, and the so-called certificate authority (CA:Certificate Authority) publish a public key certificate like the case of the high-order apparatus 20 mentioned above.
In addition, in case the public key of controlled-system apparatus (low rank apparatus) 30 and a secret key perform apparatus registration to a service center 10, they are newly good also as generation or composition which a service center generates, receives this and is stored in apparatus, and in this case, if the public key certificate is required, they will be separately acquired from a certificate authority.
Moreover, controlled-system apparatus (low rank apparatus) 30 is good also as composition whose storing of the group of two or more keys was enabled, and good also as composition which made it possible to change the group of a key for every service center which apparatus connects, and every service.
In addition, the public key of a service center 10 is beforehand recorded on the internal memory of the encryption communication IC 305 of apparatus.
In addition, in considering it as the composition only using a common key encryption system, a common key is published by the service center 10 and it stores it in the internal memory of the encryption communication IC 305 of controlled-system apparatus (low rank apparatus) 30.
In addition, corresponding to the identifier (ID) of controlled-system apparatus (low rank apparatus) 30, a service center may hold a common key.
[0063] Controlled-system apparatus (low rank apparatus) 30
Furthermore, processing control of the encryption communication IC 305, communication control through each interface,
CPU301 for controlling various processings, such as data access control of storage 309, the temporary storage of communication data,
The control unit 308 which enables directions of the communication start by the display section 303 and the user who display the directions data to the memory 302 constituted by RAM which functions as the storing section of a processing program, ROM, etc., and the user who operates apparatus etc., a hard disk, CD,

It has the storage 309 constituted with DVD etc.
[0064] Controlled-system apparatus (low rank apparatus) 30 has further the apparatus peculiar section 304 which offers the function of apparatus original.
Furthermore, you may constitute controlled-system apparatus (low rank apparatus) 30 so that data may be recorded on a memory stick and an information recording medium 310 like FD, CD, and DVD.
In that case, it has the interface 306 with the information recording medium 310.
In the off-line type case of Fig. 4, the control information from a service center 10 is received through this information recording medium 310.
With the online type composition of Fig. 3, any method becomes possible through the information recording medium 310 through a local network.
[0065] That is, in the online type of Fig. 3, in case controlled-system apparatus (low rank apparatus) 30 receives service, connect with high-order apparatus 20 using the local network interface 307, and connect it with a service center 10 using the connection capability of the external interface 206 of high-order apparatus 20.
At this time, controlled-system apparatus (low rank apparatus) 30 performs communication control uniquely.
Moreover, high-order apparatus 20 connects with a center as a substitute of controlled-system apparatus (low rank apparatus) 30, data are transmitted and received, in the off-line type of Fig. 4, controlled-system apparatus (low rank apparatus) 30 records the data on an information recording medium by high-order apparatus 20, and moves the information recording medium to controlled-system apparatus (low rank apparatus) 30, and controlled-system apparatus (low rank apparatus) 30 reads data from the information recording medium.
[0066] Although the online type of Fig. 3 mentioned above and the off-line type controlled-system apparatus (low rank apparatus) 30 of Fig. 4 have the encryption communication IC 305 and explained it as possible composition of encryption processing in addition
It is good also as composition equipped only with IC which does not encipher in low rank apparatus but controls communication, and the high-order apparatus which made off-line connection through online connection or a storage medium through the communication line in this case is able to execute encryption processing of the contents of communication by proxy.
Attestation by an apparatus identifier (ID) is performed for attestation with the controlled-system apparatus 30 in this case (low rank apparatus), and high-order apparatus 20.
[0067] The example of composition of the <service center> service center 10 is shown in Fig. 5.
A service center 10 consists of the external network interface 105 and the encryption communication IC 104, the data base 103 for service offer, the apparatus information data

base 106, the user information data base 107, CPU101, memory 102, and a data bus that connects these further.

[0068] The encryption communication IC 104 processes communication with high-order apparatus 20 and encryption of data, attestation of the apparatus for service offer, etc. The center identifier (ID) peculiar to a service center is recorded on this encryption communication IC 104, and this is used in the case of mutual recognition with each apparatus which serves as a communication partner.

[0069] Operation required in order to use a public-key crypto system and a common key encryption system is possible for the encryption communication IC 104 of a service center 10.

As for たま for communication, the information on the identifier (ID) of each [for service] apparatus, a public key, etc. is stored in the apparatus information data base 106.

In the case of the apparatus which uses a common key encryption system in data communication, Apparatus ID and the common key corresponding to it are beforehand stored in this apparatus information data base 106.

[0070] The apparatus which receives offer of the service from a service center 10 is managed in the user information data base 107, and the identifier (ID) of the user who performs payment processing of the countervalue of service etc., i.e., a service user, each user's settlement-of-accounts information, etc. are stored in it.

Data required in order to offer service are stored in the data base 103 for service offer.

CPU101 controls various processings, such as processing control of the encryption communication IC 104, communication control through each interface, and data access control of each storage, and memory 102 is constituted by RAM, ROM, etc. which function as the temporary storage of communication data, and the storing section of a processing program.

[0071] As a public-key crypto system used in the service offer system through the means of communication of [encryption / attestation level] book invention, it is possible to use code systems, such as DES, as a common key encryption system, and RSA etc. may take required intensity etc. into consideration and may use a suitable system.

[0072] Fig. 6 summarizes the connection form between the service center 10 in this invention, and high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30, and encryption / attestation level.

[0073] A service center 10 and high-order apparatus 20 are connected in the external network.

Moreover, encryption and attestation use a public-key crypto system.

There are six kinds of forms of connection between high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30.

Namely, when (1) controlled-system apparatus (low rank apparatus) 30 can connect with a local network and a public-key crypto system can be used,

(2) When controlled-system apparatus (low rank apparatus) 30 can connect with a local network and only a common key encryption system can be used,
(3) When controlled-system apparatus (low rank apparatus) 30 can connect with a local network and a code cannot be used,
(4) When data exchange is possible for controlled-system apparatus (low rank apparatus) 30 and it can use a public-key crypto system by movement of a recording medium,
(5) When data exchange is possible for controlled-system apparatus (low rank apparatus) 30 and it can use only a common key encryption system by movement of a recording medium, it is the case where data exchange is possible for (6) controlled-system apparatus (low rank apparatus) 30, and it cannot use a code by movement of a recording medium.
In addition, two or more low rank apparatus can be connected to one high-order apparatus, and communication with controlled-system apparatus (low rank apparatus) various type of high-order apparatus 20 is attained by considering it as the composition which can respond to two or more code systems.
In addition, high-order apparatus can identify a subordinate's low rank apparatus by referring to the apparatus ID of controlled-system apparatus (low rank apparatus).
[0074] Offer processing of the remote service using the service center 10 of the high-order apparatus 20 in the service offer system through the means of communication of [whole flow] book invention and controlled-system apparatus (low rank apparatus) 30 is explained below.
[0075] The figure from Fig. 7 to Fig. 10 is a flow figure having shown briefly the flow of processing until [whole] it results [from a service start] in an end.
The latter part explains the details of the processing included in these flows.
First, the outline of the flow of processing of the service offer system of this invention is explained using Figs. 7-10.
[0076] As first shown in the flow of Fig. 7, in connecting high-order apparatus 20 for the first time to a service center 10 through a network, it performs apparatus registration to the service center 10 shown in Step S701.
When the processing at the time of first connection is completed, it moves to cases, such as the processing which does not need apparatus registration, for example, free maintenance offer etc., at the step of apparatus attestation shown in Step S702.
An apparatus attestation processing flow is shown in Fig. 7.
This is a procedure to which high-order apparatus 20 and a service center 10 check a communication partner's justification mutually.
The latter part explains in detail the apparatus registration protocol and apparatus Challenge Handshake Authentication Protocol which are shown in a figure.
[0077] By performing Challenge Handshake Authentication Protocol shown in Fig. 7, inaccurate apparatus can receive service or it can prevent communicating with a service center 10 accidentally.

When apparatus attestation of Step S702 goes wrong, processing is stopped after performing error handling.
When it succeeds in apparatus attestation, user registration will be performed if required.
[0078] Register required information, such as the user information on apparatus, for example, a name, a credit card number for courtesy-rates settlement of accounts, or a bank account number, into the user information data base (107 shown in Fig. 5) of a service center 10 in the user registration procedure shown in Fig. 8 (Step S801).
Information registration (Step S802) required for user authentication, such as a password, after that is also performed.
[0079] Fig. 9 is processing the upper row indicates user information change procedure, such as user information, for example, a name, and a credit number, to be, and the lower berth is the flow which shows the change procedure of information required for user authentication, such as a password.
In user information change procedure, user authentication (Step S901) is performed first.
This is for preventing persons other than a just user changing others' user information unjustly.
When user authentication goes wrong, processing is stopped after performing error handling.
When it succeeds in user authentication, user information registration (Step S902) is performed continuously.
[0080] If registration of user information is completed, it will restrict, when required and information required for user authentication, for example, the user authentication information change procedure of a password, will be performed.
In user authentication information change procedure, user authentication is performed first.
This is for preventing persons other than a just user changing user authentication information, such as others' password, unjustly.
When user authentication goes wrong, processing is stopped after performing error handling.
When it succeeds in user authentication, user authentication information is changed continuously (Step S903).
The above procedure is completed, and in giving one's service, it performs service implementation procedure.
[0081] Execution processing of services, such as control of controlled-system apparatus and a maintenance, i.e., a service implementation procedure flow, is shown in Fig. 10.
In service implementation procedure, if required, user authentication will be performed first.
This is for preventing persons other than a just user receiving service unjustly.
Whether user authentication is performed changes with services.

When user authentication goes wrong, processing is stopped after performing error handling.
When it succeeds in user authentication, its service is given continuously.
After service is completed, when not ending connection, procedure after the time of an apparatus attestation end is performed again.
[0082] The protocol which registers [each protocol] (1) apparatus registration protocol a. high-order apparatus まず and high-order apparatus 20 to a service center 10 is explained. This protocol is a protocol for registering Apparatus ID, a model name, and an apparatus public key into the apparatus information data base of a center.
[0083] As previous Fig. 6 explained, between high-order apparatus 20 and a service center 10, mutual recognition and data communication are performed by a public-key crypto system. When the group of the public key and secret key of high-order apparatus itself [which is needed when using a public-key crypto system] is beforehand stored in the internal memory of the encryption communication IC 205 of high-order apparatus 20, when it did not store these keys in the internal memory of the encryption communication IC 205 beforehand but connection with a service center 10 is needed, apparatus registration is performed to a service center 10, and there is two composition of composition of generating each key in that case.
The protocol of the case former [whose] has been key stored is shown in Fig. 11, and the protocol in the case of generating a key is shown in Fig. 12.
[0084] Explain processing of Fig. 11 and Fig. 12.
When performing apparatus registration, high-order apparatus 20 transmits an apparatus registration start demand to a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify to apparatus that an apparatus registration start is possible.
A service center 10 transmits an own center identifier (ID) simultaneously.
[0085] High-order apparatus 20 checks a center by the service center identifier (ID) sent from a service center 10, and transmits a high-order apparatus identifier (ID), an own model name, and an own public key certificate to a service center 10.
The public key of a service center 10 is stored in the encryption communication IC 205 of high-order apparatus 20, and transmitting data are enciphered using this public key in the case of transmission to a service center 10.
[0086] In addition, like the example shown in Fig. 12, when high-order apparatus 20 self generates the group of a key, the public key which high-order apparatus 20 generated instead of the public key certificate is transmitted to a center.
[0087] Since it is enciphered with the public key of a service center 10, the transmitting data from high-order apparatus 20 to a service center 10 can eliminate a possibility that data contained in transmitting data, such as a high-order apparatus identifier (ID) and a model name, will be revealed to a third person, or will be altered.

[0088] The center which received data, such as a high-order apparatus identifier (ID), decodes the data sent from high-order apparatus with the secret key of service center 10 self.
The high-order apparatus identifier in the decoded data (ID) is verified, and if it is a just identifier (ID), the high-order apparatus identifier (ID), the model name and public key certificate, or public key in transmitting data will be registered into the apparatus information data base 106.
When the registration to a data base is completed normally, a service center 10 returns the notice of the completion of apparatus registration processing to high-order apparatus 20.
When decode of data or justification verification of a high-order apparatus identifier (ID), and the registration to a data base go wrong, a service center 10 returns the notice of an error to high-order apparatus 20.
[0089] Explain the protocol which registers b. controlled-system apparatus (low rank apparatus), next controlled-system apparatus (low rank apparatus) 30 to a service center 10.
[0090] When controlled-system apparatus (low rank apparatus) 30 performs apparatus registration, procedures differ by online type low rank apparatus and off-line type low rank apparatus.
Furthermore, the apparatus which a public-key crypto system can use differs also from the apparatus which is not made.
In addition, the high-order apparatus 20 which controlled-system apparatus (low rank apparatus) 30 connects shall carry out apparatus Challenge Handshake Authentication Protocol between high-order apparatus 20 and a service center 10, before performing this procedure, and attestation shall be made between centers.
[0091] The procedure in the case of using online type low rank apparatus for the online type low rank apparatus beginning of a b-1. public-key crypto system is shown in Fig. 13.
When a public key can be used by online type low rank apparatus, and using a public-key crypto system, are needed.
When the group of the public key and secret key of controlled-system apparatus (low rank apparatus) 30 self is beforehand stored in the internal memory of the encryption communication IC 305 of controlled-system apparatus (low rank apparatus) 30,
These keys are not stored in the internal memory of the encryption communication IC 305, but when connection with a service center 10 is needed, apparatus registration is performed to a service center 10, and there is two composition of composition of generating each key in that case.
The protocol of the case former [whose] has been key-stored is shown in Fig. 13, and the protocol in the case of generating a key is shown in Fig. 14.
[0092] Explain processing of Fig. 13 and Fig. 14.

When performing apparatus registration, controlled-system apparatus (low rank apparatus) 30 publishes an apparatus registration start demand to high-order apparatus 20 first.
The high-order apparatus 20 which received this relays an apparatus registration start demand to a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify that an apparatus registration start is possible to high-order apparatus 20.
And high-order apparatus 20 notifies that an apparatus registration start is possible to controlled-system apparatus (low rank apparatus) 30.
[0093] If this apparatus registration start confirmative advice is received, controlled-system apparatus (low rank apparatus) 30 will encipher the apparatus ID of controlled-system apparatus (low rank apparatus) itself, a model name, and a public key certificate with the public key of a center, and will transmit them to high-order apparatus.
In addition, as shown in Fig. 14, when low rank apparatus generates the group of a key, an own public key is transmitted to high-order apparatus 20 instead of a public key certificate.
The high-order apparatus 20 which received this relays these receiving data to a service center as they are.
[0094] Since it is enciphered with the public key of a service center 10, the data transmitted to high-order apparatus 20 and a service center 10 from controlled-system apparatus (low rank apparatus) 30 can eliminate a possibility that data contained in transmitting data, such as a controlled-system apparatus (low rank apparatus) identifier (ID) and a model name, will be revealed to a third person, or will be altered.
[0095] The center which received data, such as a controlled-system apparatus (low rank apparatus) identifier (ID), decodes the data sent from high-order apparatus with the secret key of service center 10 self.
The controlled-system apparatus (low rank apparatus) identifier in the decoded data (ID) is verified, and if it is a just identifier (ID), the controlled-system apparatus (low rank apparatus) identifier (ID), the model name and public key certificate, or public key in transmitting data will be registered into the apparatus information data base 106.
When the registration to a data base is completed normally, a service center 10 returns the notice of the completion of apparatus registration processing to high-order apparatus 20.
When decode of data or justification verification of a high-order apparatus identifier (ID), and the registration to a data base go wrong, a service center 10 returns the notice of an error to high-order apparatus 20.
[0096] High-order apparatus 20 relays the notice of the completion of processing or the notice of an error which received from the service center 10 to controlled-system apparatus (low rank apparatus) 30.
[0097] The online type low rank apparatus public-key crypto system of a b-2. common key encryption system cannot be used, but describe that a common key system can be used or the

apparatus registration procedure of online type low rank apparatus without an encryption function.

[0098] The protocol in this case is shown in Fig. 15.

Processing until it notifies that an apparatus registration start is possible for high-order apparatus 20 to controlled-system apparatus (low rank apparatus) 30 also in this case is the same.

If controlled-system apparatus (low rank apparatus) 30 receives apparatus registration start confirmative advice, controlled-system apparatus (low rank apparatus) 30 will transmit own Apparatus ID and an own model name to high-order apparatus 20.

[0099] Although the apparatus ID transmitted to high-order apparatus 20 in this case and model name information are not enciphered, since it is on a local network, it is thought that there are comparatively few problems of security compared with an external network.

High-order apparatus 20 enciphers the information received from controlled-system apparatus (low rank apparatus) 30 with the public key of a service center 10.

That is, high-order apparatus 20 executes encryption of data by proxy.

Since next processing is the same as that of the procedure in the case of the low rank apparatus which a public-key crypto system can use, explanation is omitted.

[0100] Describe the apparatus registration procedure in the off-line type low rank apparatus of a b-3. public-key crypto system, then off-line type low rank apparatus.

When a public-key crypto system can be used by off-line type low rank apparatus, and using a public-key crypto system, are needed.

When the group of the public key and secret key of controlled-system apparatus (low rank apparatus) 30 self is beforehand stored in the internal memory of the encryption communication IC 305 of controlled-system apparatus (low rank apparatus) 30,

These keys are not stored in the internal memory of the encryption communication IC 305, but when connection with a service center 10 is needed, apparatus registration is performed to a service center 10, and there is two composition of composition of generating each key in that case.

The protocol of the case former [whose] has been key stored is shown in Fig. 16, and the protocol in the case of generating a key is shown in Fig. 17.

[0101] Explain processing of Fig. 16 and Fig. 17.

Controlled-system apparatus (low rank apparatus) 30 attests an information recording medium first.

The information recording medium 310 is a memory card, and attestation processing using the identifier of a memory card etc. is performed.

If attestation is materialized, controlled-system apparatus (low rank apparatus) 30 will encipher a controlled-system apparatus (low rank apparatus) identifier (ID), a model name and an own public key certificate (Fig. 16), or an own public key (Fig. 17) with the public key of a service center, and will transmit it to the information recording medium 310.

[0102] After data transfer is completed, remove the information recording medium 310 from controlled-system apparatus (low rank apparatus) 30 low-rank apparatus, and equip high-order apparatus 20.
High-order apparatus 20 will start attestation of an information recording medium, if equipped with the information recording medium 211 (it is the same as the information recording medium 310).
After information recording-medium attestation is completed, high-order apparatus 20 transmits data from an information recording medium (read-out processing).
High-order apparatus 20 gives an apparatus registration start demand to a service center 10 as a substitute of controlled-system apparatus (low rank apparatus) 30 after a transmission end.
[0103] If a service center 10 is in the state which can meet the demand, it will notify that an apparatus registration start is possible to high-order apparatus 20.
And high-order apparatus 20 transmits the data transmitted from the information recording medium 211 to a center as it is.
The center which received data, such as a controlled-system apparatus (low rank apparatus) identifier (ID) read from the information recording medium 211, decodes the data which high-order apparatus 20 relayed with the own secret key.
The controlled-system apparatus (low rank apparatus) identifier in the data decoded after that (ID) is verified, and if it is just ID, the received controlled-system apparatus (low rank apparatus) identifier (ID), the model name and public key certificate (Fig. 16), or public key (Fig. 17) will be registered into the apparatus information data base 106.
When the registration to a data base is completed normally, a service center 10 returns the notice of the completion of processing to high-order apparatus 20.
When decode of data or justification verification of a controlled-system apparatus (low rank apparatus) identifier (ID), and the registration to a data base go wrong, a service center 10 returns the notice of an error to high-order apparatus 20.
High-order apparatus 20 transmits the notice of the completion of processing, or the notice of an error to the information recording medium 211.
Then, the information recording medium 211 is moved to controlled-system apparatus (low rank apparatus) 30 from high-order apparatus 20.
Controlled-system apparatus (low rank apparatus) 30 transmits the notice from a service center 10 from an information recording medium, after performing information recording-medium attestation.
If the contents of a notice are the notices of an error, apparatus registration will be tried again.
[0104] The off-line type low-rank apparatus public-key crypto-system of a b-4. common key encryption system cannot be used, but describe that a common key system can be used or the apparatus registration procedure of off-line type low rank apparatus without an encryption function.

The protocol in this case is shown in Fig. 18.
Controlled-system apparatus (low rank apparatus) 30 attests the information recording medium 310 first.
Then, controlled-system apparatus (low rank apparatus) 30 transmits own Apparatus ID and an own model name to the information recording medium 310.
After transmission is completed, the information recording medium 310 is removed from controlled-system apparatus (low rank apparatus) 30, and high-order apparatus 20 is equipped.
[0105] High-order apparatus 20 will start attestation of the information recording medium 211, if equipped with the information recording medium 211 (= information recording medium 310).
After attestation of the information recording medium 211 is completed, high-order apparatus 20 transmits data from the information recording medium 211.
High-order apparatus 20 transmits an apparatus registration start demand to a service center 10 after a transmission end.
If a service center 10 is in the state which can meet the demand, it will notify that an apparatus registration start is possible to high-order apparatus 20.
High-order apparatus 20 enciphers the data transmitted from the information recording medium 211 with the public key of a service center 10, and transmits them to a center.
The center which received data, such as a controlled-system apparatus (low rank apparatus) identifier (ID) read from the information recording medium 211, decodes the data which high-order apparatus 20 relayed with the own secret key.
The controlled-system apparatus (low rank apparatus) identifier in the data decoded after that (ID) is verified, and if it is just ID, the controlled-system apparatus (low rank apparatus) identifier (ID) and model name which were received will be registered into the apparatus information data base 106.
Processing of the subsequent notice of the completion of processing etc. is the same as that of the case where the off-line type low rank apparatus which a public-key crypto system can use is used.
[0106] The details of the apparatus Challenge Handshake Authentication Protocol performed in [apparatus Challenge Handshake Authentication Protocol] next a service center 10, high-order apparatus 20, and both controlled-system apparatus (low rank apparatus) 30 are explained.
Apparatus Challenge Handshake Authentication Protocol is a process performed in order to check a communication partner's justification among 2 persons who perform data communication.
The composition which performs generation of a session key at the time of mutual recognition processing, performs encryption processing by using the generated session key as a share key, and performs data transmission is one desirable data transfer method.

Hereafter, the apparatus Challenge Handshake Authentication Protocol performed centering on high-order apparatus 20 and the apparatus Challenge Handshake Authentication Protocol performed centering on controlled-system apparatus (low rank apparatus) 30 are explained, respectively.

[0107] Explain the apparatus Challenge Handshake Authentication Protocol which checks the mutual justification performed between a. high-order apparatus まず, high-order apparatus 20, and a service center 10.

[0108] A protocol in case a service center 10 and high-order apparatus 20 perform apparatus attestation is shown in Fig. 19.

High-order apparatus 20 transmits an apparatus attestation start demand to a service center 10 first.

If a service center 10 is in the state which can meet the demand, it will notify to apparatus that an apparatus attestation start is possible.

Under the present circumstances, a service center 10 transmits the own center ID.

[0109] High-order apparatus 20 will transmit the apparatus ID of high-order apparatus 20 self, if the response in which an attestation start is possible is received from a service center 10.

Then, mutual recognition is performed between a service center 10 and high-order apparatus 20.

As a procedure of mutual recognition, the procedure shown, for example in ISO9798 can be used.

[0110] Explain the mutual recognition method using the elliptic curve cryptosystem of the 160 bit length which is a public-key crypto system as a mutual recognition procedure of ISO9798 using Fig. 20.

In Fig. 20, although ECC is used as a public-key crypto system, as long as it is the same public-key crypto system, any are sufficient.

Moreover, key size may not be 160 bits, either.

In Fig. 20, one side of A and B is equivalent to a service center 10, and another side is equivalent to high-order apparatus 20.

[0111] First, B generates the 64-bit random number Rb, and transmits to A.

A which received this newly generates the 64-bit random number Ra and the random number Ak smaller than the number p of marks.

And point Av=AkxG as for which Ak doubled the base point G is calculated, electronic signature A.Sig to Ra, Rb, and Av (X coordinates and Y coordinates) is generated, and B is returned with the public key certificate of A.

Here, since 64 bits, and X coordinates and Y coordinates of Av are 160 bits, Ra and Rb generate the electronic signature to a total of 448 bits, respectively.

[0112] In case a public key certificate is used, using the public key of the public key certificate certificate authority (CA) which self holds, a user verifies the electronic

signature of the public key certificate concerned, and after he succeeds in verification of electronic signature, he picks out a public key from a public key certificate.
[0113] B which received the public key certificate of A, Ra, Rb and Av, and electronic signature A.Sig verifies whether Rb which A has transmitted is in agreement with what B generated.
As a result, when in agreement, the electronic signature in the public key certificate of A is verified with the public key of a certificate authority, and the public key of A is taken out.
And electronic signature A.Sig is verified using the taken-out public key of A.
After succeeding in verification of electronic signature, B attests A as a just thing.
[0114] Next, B generates the random number Bk smaller than the number p of marks.
And point Bv=BkxG as for which Bk doubled the base point G is calculated, electronic signature B.Sig to Rb, Ra, and Bv (X coordinates and Y coordinates) is generated, and A is returned with the public key certificate of B.
[0115] A which received the public key certificate of B, Rb, Ra and Av, and electronic signature B.Sig verifies whether Ra which B has transmitted is in agreement with what A generated.
As a result, when in agreement, the electronic signature in the public key certificate of B is verified with the public key of a certificate authority, and the public key of B is taken out.
And electronic signature B.Sig is verified using the taken-out public key of B.
After succeeding in verification of electronic signature, A attests B as a just thing.
[0116] When both succeed in attestation, B calculates BkxAv (although Bk is a random number, since Av is a point on an elliptic curve, scalar twice calculation of the point on an elliptic curve is required for it), and A calculates AkxBv, and use it for communication after using 64 bits of low ranks of X coordinates of these points as a session key (when a common key encryptosystem is made into the common key encryptosystem of 64-bit key length).
Of course, a session key may be generated from Y coordinates and you may not be 64 bits of low ranks.
In addition, transmitting data are not only enciphered with a session key, but electronic signature may be attached in the secret communication after mutual recognition.
[0117] When injustice and disagreement are found on the occasion of verification of electronic signature, or verification of receiving data, interrupt processing as that in which mutual recognition failed.
[0118] The disclosure of communication data to a third person is prevented by enciphering transmitting data and performing data communication mutually using the session key generated in such mutual recognition processing.
In addition, whichever of a service center 10 and high-order apparatus 20 may perform generation of a session key required for encryption of data.

When exchange of mutual recognition and a session key goes wrong, a service center 10 returns an error to high-order apparatus 20.
If all processings are completed, a center will notify the completion of processing to high-order apparatus.
[0119] b-1. online type low rank apparatus -- describe the case where a service center 10 and online type controlled-system apparatus (low rank apparatus) 30 next perform apparatus attestation.
The protocol in this case is shown in Fig. 21.
[0120] Online type controlled-system apparatus (low rank apparatus) 30 transmits an apparatus attestation start demand to high-order apparatus 20 first.
If high-order apparatus 20 is in the state which can meet the demand, it will notify that an apparatus attestation start is possible to controlled-system apparatus (low rank apparatus) 30.
Controlled-system apparatus (low rank apparatus) 30 transmits own apparatus ID to high-order apparatus 20.
And mutual recognition is performed between high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30.
[0121] In addition, mutual recognition between high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30 may be performed as attestation processing of the public-key crypto system of Fig. 20 explained as mutual recognition processing between the above-mentioned service center 10 and high-order apparatus 20, and may perform mutual recognition by a common key encryption system.
[0122] The mutual recognition method using a common key encryption system is explained using Fig. 22.
Although Fig. 22 is the example which used DES as a common key encryption system, the other methods are also applicable if it is the same common key encryption system.
In Fig. 22, A or B corresponds to high-order apparatus 20, and another side corresponds to controlled-system apparatus (low rank apparatus) 30.
[0123] First, B generates the random number Rb which is 64 bits, and transmits ID (b) which is Rb and self ID to A.
A which received this newly generates the 64-bit random number Ra, in order of Ra, Rb, and ID (b), Key Kab is used for it in the CBC mode of DES, it enciphers data, and returns them to B.
[0124] B which received this decrypts receiving data with Key Kab.
First, the decryption method of receiving data decrypts a cryptogram E1 with Key Kab, and obtains a random number Ra.
Next, a cryptogram E2 is decrypted with Key Kab, the exclusive OR of the result and E1 is carried out, and Rb is obtained.
Finally, a cryptogram E3 is decrypted with Key Kab, the exclusive OR of the result and E2 is carried out, and ID (b) is obtained.

In this way, Rb and ID (b) verify whether it is in agreement with what B transmitted among Ra, Rb(s), and ID (b) which were obtained.
When it passes in this verification, B attests A as a just thing.
[0125] Next, B generates the session key (Session Key (hereafter referred to as Kses)) used after attestation (a random number is used for the generation method).
And in order of Rb, Ra, and Kses, in the CBC mode of DES, Key Kab is used, it enciphers, and A is returned.
[0126] A which received this decrypts receiving data with Key Kab.
Since the decryption method of receiving data is the same as that of decryption processing of B, details are omitted here.
In this way, Rb and Ra verify whether it is in agreement with what A transmitted among Rb(s), Ra, and Kses(es) which were obtained.
When it passes in this verification, A attests B as a just thing.
After attesting the partner of each other, the session key Kses is used as a common key for the secret communication after attestation.
[0127] In addition, when injustice and disagreement are found on the occasion of verification of receiving data, processing is interrupted as that in which mutual recognition failed.
[0128] If mutual recognition is successful, high-order apparatus 20 will require an apparatus attestation start as a substitute of controlled-system apparatus (low rank apparatus) 30 from a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify that an apparatus attestation start is possible to high-order apparatus 20.
High-order apparatus 20 transmits the apparatus ID of controlled-system apparatus (low rank apparatus) 30 to a service center 10.
A service center 10 verifies the justification of the apparatus ID of low rank apparatus here.
Verification of justification is performed as processing which confirms whether the apparatus ID contained in sending data is registered into the apparatus information data base 106 which a service center 10 has.
After justification verification of Apparatus ID is completed normally, high-order apparatus 20 gives permission of the direct communication with a service center 10 to controlled-system apparatus (low rank apparatus) 30.
High-order apparatus 20 does not participate in the contents of communication between a service center 10 and controlled-system apparatus (low rank apparatus) 30 after this.
[0129] In response to direct communication permission with a service center 10, controlled-system apparatus (low rank apparatus) 30 communicates a center and directly, and performs mutual recognition.
Mutual recognition is performed using either of the examples of above-mentioned Figs. 20 or 22.

Completion of mutual recognition enciphers, transmits and receives data using the session key (common key) generated at the time of future mutual recognition.
Whichever of a service center 10 and controlled-system apparatus (low rank apparatus) 30 may perform generation of a session key.
In addition, since mutual recognition is completed here, respectively between a service center 10 and high-order apparatus 20 and between high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30, it is also possible to omit the direct mutual recognition of a service center 10 and controlled-system apparatus (low rank apparatus) 30.
When exchange of mutual recognition and a session key goes wrong, a center returns an error to low rank apparatus.
If all processings are completed, a service center 10 will notify the completion of processing to controlled-system apparatus (low rank apparatus) 30.
If a session key can share between controlled-system apparatus (low rank apparatus) 30 and a service center 10, online type low rank apparatus can be treated like high-order apparatus 20 in each procedure explained henceforth.
[0130] In addition, in the case of controlled-system apparatus (low rank apparatus) 30 without an encryption function, attestation of controlled-system apparatus (low rank apparatus) 30 is performed by attestation processing which used the one-time password.
In this case, a service center 10 or high-order apparatus 20 generates and holds a session key, and makes data communication between the service center 10 through an external network, and high-order apparatus 20 the data communication using a session key.

The protocol in this case is shown in Fig. 23.
[0131] Explain the apparatus Challenge Handshake Authentication Protocol of b-2. off-line type low rank apparatus, next off-line type low rank apparatus.
The protocol in this case is shown in Fig. 24.
Off-line type controlled-system apparatus (low rank apparatus) 30 is the composition of receiving control information through information recording media, such as memory card, as explained previously.
[0132] If low rank apparatus is not first equipped with the information recording medium, equip with off-line type controlled-system apparatus (low rank apparatus) 30.
In that case, a recording medium is attested.
This attestation processing is performed by the method using the above-mentioned symmetrical key, an asymmetrical key, and a password etc. according to the composition (a scrambling function, key storing composition) of controlled-system apparatus (low rank apparatus) 30 and an information recording medium.
If recording-medium attestation is successful, controlled-system apparatus (low rank apparatus) 30 will transmit data required for apparatus attestation of Apparatus ID etc. to an information recording medium.

An end of transmission moves an information recording medium to high-order apparatus 20.
[0133] If an information recording medium is set, high-order apparatus 20 will transmit data required for apparatus attestation from a medium, after attesting an information recording medium.
Attestation processing of an information recording medium is performed by the method using the above-mentioned symmetrical key, an asymmetrical key, and a password etc. like attestation processing with controlled-system apparatus (low rank apparatus) 30 and an information recording medium.
An end of transmission performs mutual recognition of high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30 based on the storing data of an information recording medium.
In the meantime, if it needs to be moved between the high-order apparatus 20 of an information recording medium, and controlled-system apparatus (low rank apparatus) 30, it will carry out.
If mutual recognition is successful, high-order apparatus 20 will require an apparatus attestation start of a service center 10 instead of controlled-system apparatus (low rank apparatus) 30.
If a service center 10 is in the state which can meet the demand, it will notify that an apparatus attestation start is possible to high-order apparatus 20.
[0134] Next, high-order apparatus 20 transmits the apparatus ID of controlled-system apparatus (low rank apparatus) 30 to a service center 10.
A service center 10 verifies the justification of the apparatus ID of controlled-system apparatus (low rank apparatus) 30 here.
If justification verification of Apparatus ID is completed normally, controlled-system apparatus (low rank apparatus) 30 will perform exchange of a service center 20, mutual recognition processing, and a session key.
However, since controlled-system apparatus (low rank apparatus) 30 and a service center 10 cannot carry out direct communication, high-order apparatus 20 and an information recording medium intervene, and they are performed.
In the meantime, movement between the high-order apparatus 20 of an information recording medium and controlled-system apparatus (low rank apparatus) 30 is performed if needed.
Completion of mutual recognition generates a session key (common key) required for encryption of future data.
Whichever of a service center 10 and controlled-system apparatus (low rank apparatus) 30 may perform generation of a session key.
In addition, in the case of controlled-system apparatus (low rank apparatus) 30 without an encryption function, attestation of controlled-system apparatus (low rank apparatus) 30 is performed by attestation processing which used the one-time password.
In this case, a service center 10 or high-order apparatus 20 generates and holds a session key, and makes data communication between the service center 10 through an external

network, and high-order apparatus 20 the data communication using a session key.

When exchange of mutual recognition and a session key goes wrong, a service center 10 returns an error to high-order apparatus 20.
If all processings are completed, a service center 10 will notify the completion of processing to high-order apparatus 20.
High-order apparatus 20 transmits the notice of the completion of processing, or the notice of an error to an information recording medium.
If an information recording medium is moved to controlled-system apparatus (low rank apparatus) 30, controlled-system apparatus (low rank apparatus) 30 will attest an information recording medium, and will transmit the notice of the completion of processing, or the notice of an error from a recording medium (read-out processing).
[0135] The user registration for registering user information, such as [user registration and an information change protocol], next a user name, settlement-of-accounts information, into the user information data base 107 (referring to Fig. 5) of a service center 10 and an information change protocol are explained.
[0136] Describe the processing in the case of a. high-order apparatus, online type low rank apparatus まず high-order apparatus 20, and online type controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 25.
High-order apparatus 20 and online type controlled-system apparatus (low rank apparatus) 30 are named "apparatus" generically.
Apparatus performs the start demand of user registration to a service center 10.
If a service center 10 is in the state where user information registration can be performed, it will notify a start check to apparatus.
Apparatus enciphers the user information which the user inputted with a session key, and transmits it with Apparatus ID.
User information is a name, the address, settlement-of-accounts information, etc.
Settlement-of-accounts information is information required for settlement of onerous services, such as a bank account, a credit card number, and a prepaid card number.
A service center 10 decodes the enciphered user information with the session key corresponding to Apparatus ID.
[0137] A service center 10 publishes User ID to the user concerned continuously, and a service center 10 registers the user ID and user information, and Apparatus ID into the inner user information data base 107.
After registration of the user information on a data base, a service center 10 enciphers User ID with a session key, and transmits him to apparatus.
Apparatus will decode the enciphered user ID with a session key, if this is received.
And a user is notified of User ID.

A notice is performed in the display section 303 (refer to Fig. 3) of controlled-system apparatus (low rank apparatus) 30.
In addition, displaying in high-order apparatus is also possible.
In order to save the time and effort which inputs User ID whenever a user uses apparatus here, it is very good in the way save User ID to apparatus and a user chooses his ID.
Finally a service center 10 performs the notice of the completion of processing, or the notice of an error to apparatus.
[0138] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it enciphers, transmits and receives data and high-order apparatus 20 enciphers data with a session key, it transmits to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to low rank apparatus.
The protocol in this case is shown in Fig. 26.
[0139] User information is still more nearly already registered into the user information data base 107 in a service center 10, and in changing the information, publishing User ID in registration procedure and the processing which notifies User ID to high-order apparatus become unnecessary.
Moreover, instead of inputting the name for specifying a user etc., you may input the published user ID.
If the apparatus ID of the apparatus by which the user uses the service center 10 at this time is not related with the user ID of this 該, processing which adds Apparatus ID to the user information data base 107 is performed.
Other portions are the same as that of the case of user information registration.
The protocol in this case is shown in Fig. 27.
[0140] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 28.
[0141] Describe the case of b. off-line type low rank apparatus, then off-line type low rank apparatus.
The protocol in this case is shown in Fig. 29.
It equips, if off-line type controlled-system apparatus (low rank apparatus) 30 is not equipped with the recording medium.
In that case, attestation of a recording medium is needed.

After controlled-system apparatus (low rank apparatus) 30 enciphers the user information which the user inputted with a session key, it is transmitted to an information recording medium with Apparatus ID.
After transmission is completed, an information recording medium is removed from controlled-system apparatus (low rank apparatus) 30, and high-order apparatus 20 is equipped.
[0142] High-order apparatus 20 will start attestation of an information recording medium, if equipped with an information recording medium.
After attestation of an information recording medium is completed, high-order apparatus 20 transmits data from an information recording medium (reading).
High-order apparatus 20 gives a user registration start demand to a service center 10 as a substitute of low rank apparatus after a transmission end.
If a service center 10 is in the state where user information registration can be performed, it will notify a start check to high-order apparatus 20.
[0143] High-order apparatus 20 transmits the data from controlled-system apparatus (low rank apparatus) 30 to a service center 10 as it is.
A service center 10 decodes the enciphered user information with the session key corresponding to Apparatus ID.
Then, User ID is published to the user concerned and the user ID and user information, and Apparatus ID are registered into the user information data base 107.
[0144] A service center 10 enciphers User ID after registration of the user information on a data base with a session key with controlled-system apparatus (low rank apparatus) 30, and transmits him to high-order apparatus 20.
And a service center 10 performs the notice of the completion of processing, or the notice of an error to high-order apparatus 20.
The user ID enciphered as high-order apparatus 20 receives the notice of the completion of processing from a service center 10 is transmitted to an information recording medium.
Then, an information recording medium is moved to controlled-system apparatus (low rank apparatus) 30 from high-order apparatus 20.
If controlled-system apparatus (low rank apparatus) 30 is equipped with an information recording medium, controlled-system apparatus (low rank apparatus) 30 will attest an information recording medium.
If attestation is successful, controlled-system apparatus (low rank apparatus) 30 will transmit the data in an information recording medium (data reading).
[0145] Next, controlled-system apparatus (low rank apparatus) 30 decodes the enciphered user ID who read in the information recording medium with a session key.
And a user is notified of User ID.
A notice is performed in the display section 303 (refer to Fig. 4) of controlled-system apparatus (low rank apparatus) 30.

In order to save the time and effort which inputs User ID whenever a user uses apparatus here, it is very good in the way save User ID to apparatus and a user chooses his ID for it.

[0146] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.

After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.

The protocol in this case is shown in Fig. 30.

[0147] User information is still more nearly already registered into the user information data base 107 in a service center 10, and in changing the information, publishing User ID in registration procedure and the processing which notifies User ID to high-order apparatus become unnecessary.

Moreover, instead of inputting the name for specifying a user etc., you may input the published user ID.

If the apparatus ID of the apparatus by which the user uses the service center 10 at this time is not related with the user ID of this 該, processing which adds Apparatus ID to the user information data base 107 is performed.

Other portions are the same as that of the case of user information registration.

The protocol in this case is shown in Fig. 31.

[0148] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.

After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.

The protocol in this case is shown in Fig. 32.

[0149] In order to identify a [user authentication information registration protocol] user, some methods can be considered, but the case where the method and ID card which used the password here are used is explained.

When using an ID card, it is possible to use the card equipped with the mechanism in which living body information which embedded ID according to individual, such as a card and a fingerprint, can be recognized, or the card which saves the group of the public key and secret key of a user individual.

You may use whichever of the contacted type card which has a magnetic tape as an ID card, and the noncontact card which performs wireless communications.

Moreover, as a place which compares by saving the user authentication information for identifying a user, apparatus (high-order apparatus and controlled-system apparatus (low rank apparatus)) or a service center can be considered.

When saving to apparatus, it is easy to manage restriction of a user in apparatus etc. individually.
In registering with a service center, when using two or more apparatus, it is not necessary to do registration work for every apparatus.
A password etc. describes first the procedure which registers the information for attestation into apparatus or a center.
[0150] It is the method of comparing with the user authentication information which saved user authentication information, such as a preservation user's password, in the inside of apparatus, and the user inputted into a. apparatus on the occasions, such as offer of service.
In this case, registration of the password which can be set is explained.
The protocol in this case is shown in Fig. 33.
If the user ID whom the user inputted is received, the input of a password will be urged to apparatus to a user.
[0151] If a user enters a password from a control unit (in the case [In the case of high-order apparatus] of a control unit 209 and low rank apparatus control unit 308), apparatus saves the group of the password which corresponds with User ID in the memory inside apparatus.
At this time, you may encipher by not saving a password with 平文.
Next, a service center 10 notifies the completion of processing, or an error to apparatus.
[0152] Explain user authentication information registration processing in which an ID card is used next.
The protocol in this case is shown in Fig. 34.
Apparatus will transmit User ID and user authentication information from an ID card, if a user sets an ID card.
Apparatus saves the user authentication information which corresponds with User ID in the memory inside apparatus.
Next, a service center 10 notifies the completion of processing, or an error to apparatus.
[0153] It is the method of comparing with the user authentication information which saved preservation (high-order apparatus and online type low rank apparatus) user authentication information in the b. center in the service center 10, and the user inputted on the occasions, such as offer of service.
In this case, registration of the password which can be set is explained.
The protocol in this case is shown in Fig. 35.
[0154] It is as follows when using high-order apparatus and online type controlled-system apparatus (low rank apparatus) first.
Apparatus requires the registration start of user authentication information of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify to apparatus that a registration start is possible.

If the user ID whom the user inputted is received, the input of a password will be urged to apparatus to a user.
If a user enters a password, apparatus will encipher the group of the password which corresponds with User ID with a session key, and will transmit it to a service center 10 with Apparatus ID.
A service center 10 decodes User ID and the password which were enciphered with the session key corresponding to Apparatus ID.
Then, a password is registered into the user information data base 107.
When decode with a session key and the registration to a data base go wrong, a service center 10 returns an error to apparatus.
If all processings are completed, a service center 10 will notify the completion of processing to apparatus.
[0155] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 36.
[0156] Next, explain how to use an ID card.
The protocol in this case is shown in Fig. 37.
Apparatus will transmit User ID and user authentication information from an ID card, if a user sets an ID card.
Apparatus requires the registration start of user authentication information of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify to apparatus that a registration start is possible.
Then, apparatus enciphers the group of user authentication information which corresponds with User ID with a session key, and transmits it to a service center 10 with Apparatus ID.
The following processings are the same as that of the case where a password is used.
[0157] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 38.

[0158] c. off-line type low rank apparatus — describe the user authentication information registration protocol in the case of off-line type controlled-system apparatus (low rank apparatus) below.
First, registration of the password which can be set in this case is explained.
The protocol in this case is shown in Fig. 39.
[0159] Off-line type controlled-system apparatus (low rank apparatus) 30 demands the input of User ID and a password from a user.
If User ID and a password are entered, controlled-system apparatus (low rank apparatus) 30 will encipher this with a session key, and will transmit it to an information recording medium with Apparatus ID.
If an information recording medium is moved from low rank apparatus to high-order apparatus, high-order apparatus 20 will attest an information recording medium.
If attestation of an information recording medium is successful, high-order apparatus 20 will transmit data from an information recording medium.
Then, high-order apparatus 20 requires the registration start of user authentication information of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify that a registration start is possible to high-order apparatus 20.
High-order apparatus 20 transmits the data transmitted from the information recording medium (read-out) to a center as it is.
A service center 10 decodes User ID and the password which were enciphered with the session key corresponding to Apparatus ID.
Then, a password is registered into the user information data base 107.
When decode with a session key and the registration to a data base go wrong, a service center 10 returns an error to high-order apparatus 20.
If all processings are completed, a service center 10 will notify the completion of processing to high-order apparatus 20.
The notice of an error and the notice of the completion of processing to high-order apparatus 20 are transmitted to off-line type controlled-system apparatus (low rank apparatus) 30 through an information recording medium from a service center 10.
[0160] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 40.
[0161] Next, explain the user authentication information registration protocol using an ID card.
The protocol in this case is shown in Fig. 41.

Controlled-system apparatus (low rank apparatus) 30 will transmit User ID and user authentication information from an ID card, if a user sets an ID card.
The following processings are the same as that of the case where a password is used.
[0162] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 42.
[0163] The procedure which attests a user is described using the user authentication information registered by the [user authentication protocol], next the user authentication information registration protocol.
[0164] Save user authentication information to a. apparatus, save a preservation user's user authentication information to apparatus, and explain the method of the user authentication in the case of comparing with the user authentication information which the user inputted on the occasions, such as offer of service.
[0165] The protocol in the case of using a password as user authentication information is shown in Fig. 43.
If the user ID whom the user inputted is received, the input of a password will be urged to apparatus to a user.
If a user enters a password, apparatus will compare the password which selected the password corresponding to User ID and was entered as this out of the group of the User ID and the password which are saved in memory.
If it succeeds in collation, a user can say that he has just authority, and it becomes possible to receive service etc.
Error handling is performed when collation goes wrong.
[0166] Explain how to use an ID card next.
The protocol in this case is shown in Fig. 44.
Apparatus will transmit User ID and user authentication information from an ID card, if a user sets an ID card.
Then, apparatus selects the user authentication information corresponding to User ID from the groups of user authentication information with the user ID saved in internal memory, and compares the user authentication information transmitted from the ID card.
If it succeeds in collation, a user can say that he has just authority, and it becomes possible to receive service etc.
Error handling is performed when collation goes wrong.
[0167] Save user authentication information in the b. center, save a preservation user's password in a service center 10, and explain the method of the user authentication in the

case of comparing with the password which the user entered on the occasions, such as offer of service.
The protocol in the case of using a password is shown in Fig. 45.
Apparatus requires a user authentication start of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify to apparatus that an attestation start is possible.
If the user ID whom the user inputted is received, the input of a password will be urged to apparatus to a user.
If a user enters a password, apparatus will be transmitted to a center with Apparatus ID, after enciphering the group of the password which corresponds with User ID with a session key.
A center decodes User ID and the password which were enciphered with the session key corresponding to Apparatus ID.
A service center 10 compares the password registered into apparatus and the user information data base 107, and the password transmitted from apparatus.
A service center 10 transmits a collation result to apparatus.
If it succeeds in collation, a user can say that he has just authority, and it becomes possible to receive service etc.
It adds, when the apparatus ID transmitted to the entry of the user ID of the user information data base 107 concerned is not contained.
Also when a user uses two or more apparatus by this, it is possible to associate User ID and Apparatus ID.
Error handling is performed when collation goes wrong.
[0168] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 46.
[0169] Next, explain the method of user authentication using an ID card.
The protocol in this case is shown in Fig. 47.
Apparatus will transmit User ID and user authentication information from an ID card, if a user sets an ID card.
Apparatus requires a user authentication start of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify to apparatus that an attestation start is possible.
Apparatus is transmitted to a service center 10 with Apparatus ID, after enciphering the group of user authentication information which corresponds with User ID with a session key.

A service center 10 decodes User ID and the user authentication information which were enciphered with the session key corresponding to Apparatus ID.
A service center 10 compares the user authentication information registered into the user information data base 107, and the user authentication information transmitted from apparatus.
Furthermore, a service center 10 transmits a collation result to apparatus.
If it succeeds in collation, a user can say that he has just authority, and it becomes possible to receive service etc.
It adds, when the apparatus ID transmitted to the entry of the user ID of the user information data base 107 concerned is not contained.
Error handling is performed when collation goes wrong.
[0170] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 48.
[0171] In the case of c. off-line type low rank apparatus, explain the method of the user authentication in the case of off-line type controlled-system apparatus (low rank apparatus) 30 below.
The protocol in the case of using a password is shown in Fig. 49.
Off-line type controlled-system apparatus (low rank apparatus) 30 demands the input of User ID and a password from a user.
If User ID and a password are entered, controlled-system apparatus (low rank apparatus) 30 will encipher this with a session key, and will transmit it to an information recording medium with Apparatus ID.
[0172] If an information recording medium is moved from controlled-system apparatus (low rank apparatus) 30 to high-order apparatus 20, high-order apparatus 20 will attest an information recording medium.
If attestation of an information recording medium is successful, high-order apparatus 20 will transmit data from an information recording medium (reading).
And high-order apparatus 20 requires a user authentication start of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify that an attestation start is possible to high-order apparatus 20.
If a notice is received, high-order apparatus 20 will transmit the data transmitted from the information recording medium to a service center 10 as it is.
A service center 10 decodes User ID and the password which were enciphered with the session key corresponding to Apparatus ID.

A service center 10 compares the user authentication information registered into the user information data base 107, and the user authentication information transmitted from apparatus.
A service center 10 transmits a collation result to high-order apparatus 20.
If it succeeds in collation, a user can say that he has just authority, and it becomes possible to receive service etc.
It adds, when the apparatus ID transmitted to the entry of the user ID of a user information data base concerned is not contained.
Error handling is performed when collation goes wrong.
The high-order apparatus 20 which received the attestation result transmits the result to an information recording medium.
If an information recording medium is moved from high-order apparatus 20 to controlled-system apparatus (low rank apparatus) 30, controlled-system apparatus (low rank apparatus) 30 will attest an information recording medium.
If recording-medium attestation is successful, low rank apparatus will transmit data from an information recording medium (reading).
Controlled-system apparatus (low rank apparatus) 30 notifies a user of an attestation result through the display section 303.
[0173] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30 through an information recording medium.
The protocol in this case is shown in Fig. 50.
[0174] Explain the method of user authentication using the ID card in the case of off-line type controlled-system apparatus (low rank apparatus) 30 below.
The protocol in this case is shown in Fig. 51.
Off-line type controlled-system apparatus (low rank apparatus) 30 will transmit User ID and user authentication information from an ID card, if a user sets an ID card.
The following processings are the same as that of the case where a password is used.
[0175] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30 through an information recording medium.
The protocol in this case is shown in Fig. 52.

[0176] Offer processing of a [service protocol], next the remote service which used high-order apparatus 20 from the service center 10 is explained.
[0177] a. center high-order apparatus and center high-order apparatus-low rank apparatus (online) -- the protocol in the case of using a service center 10, high-order apparatus 20, and online type controlled-system apparatus (low rank apparatus) 30 is first shown in Fig. 53.
Here, when it is called apparatus, it is the general term containing high-order apparatus 20 and online type controlled-system apparatus (low rank apparatus) 30.
[0178] Apparatus requires a service start of a service center 10 first.
If a service center 10 is in the state which can meet the demand, it will notify to apparatus that a service start is possible.
Service is carried out by communicating data between a service center 10 and apparatus.
The case where the data for service offer are transmitted from a service center 10 is described.
[0179] Data for service like maintenance information are first sent to the encryption communication IC 104 from the data base 103 for service offer by control of CPU101 of a service center, for example.
The encryption communication IC 104 transmits to an external network via the external network interface 105, after enciphering with the session key exchanged between a service center and apparatus on the occasion of apparatus attestation of the data.
[0180] In the high-order apparatus 20 side, the encryption communication IC 205 decodes the data received by the external network interface 208 course using a session key.
The decoded data are transmitted to the recording devices 210, such as memory 202 and a disk, through a data bus.
CPU201 reads data from the recording devices 210, such as memory 202 and a disk, and controls the apparatus peculiar section 204.
In addition, when controlling online type controlled-system apparatus (low rank apparatus) 30, data are transmitted between high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30.
[0181] Describe the case where data are continuously transmitted to a service center 10 from online type controlled-system apparatus (low rank apparatus) 30.
First, data are sent to the encryption communication IC 305 by control of CPU301 of online type controlled-system apparatus (low rank apparatus) 30.
The encryption communication IC 305 transmits to high-order apparatus 20 through the local interface 307, after giving encryption with the session key of data.
High-order apparatus 20 transmits the data received through the local interface 208 from controlled-system apparatus (low rank apparatus) 30 to an external network via the external network interface 208.
[0182] In the service center 10 side, the encryption communication IC 104 decodes the data received by the external network interface 105 course using a session key.

The decoded data are transmitted to memory 102, the data base 103 for service offer, the apparatus information data base 106, and the user information data base 107 through a data bus.
While offering service, if required, CPU101 of a service center 10 will record fee collection information on memory 102 or the user information data base 107.
Fee collection information is the number of times of use of onerous service, time, the amount of transceiver data, etc.
[0183] Above, as explained, since it is enciphered using the session key, the protection of the contents of communication of the communication of data performed between a service center 10 and apparatus during offer of service is attained.
If offer of service is completed, CPU101 of a service center 10 will acquire a user's settlement-of-accounts information from a user data base by using User ID as a search key, and will perform settlement-of-accounts processing.
End processing is performed in case offer of service is ended.
[0184] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30.
The protocol in this case is shown in Fig. 54.
[0185] Explain offer processing of the remote service to 2. center high-order apparatus-low rank apparatus (off-line), next off-line type low rank apparatus.
In this case, service communicates between a service center 10 and high-order apparatus 20, high-order apparatus 20 receives data instead of off-line type controlled-system apparatus (low rank apparatus) 30, and it saves them once, and is carried out by gathering that data using an information recording medium, and transmitting to low rank apparatus.
The protocol in this case is shown in Fig. 55.
[0186] If controlled-system apparatus (low rank apparatus) 30 is not first equipped with the information recording medium, equip.
In that case, attestation of an information recording medium is needed.
If attestation of an information recording medium is successful, a service name, a parameter, etc. will transmit controlled-system apparatus (low rank apparatus) 30 through data required for a service start.
After transmission is completed, an information recording medium is moved to high-order apparatus 20.
[0187] If an information recording medium is set, high-order apparatus 20 will transmit data required for a service start from an information recording medium, after performing information recording-medium attestation.

After transmission is completed, high-order apparatus 20 requires a service start of a service center 10.
If a service center 10 is in the state which can meet the demand, it will notify that a service start is possible to high-order apparatus 20.
[0188] Describe the case where data are exchanged between high-order apparatus 20 and controlled-system apparatus (low rank apparatus) 30, during service offer.
If recording-medium attestation is not settled when high-order apparatus 20 transmits data to an information recording medium, the encryption communication IC 205 of high-order apparatus 20 starts attestation of an information recording medium.
If an information recording medium can be attested, CPU201 of high-order apparatus 20 will read the data received from the service center 10 for controlled-system apparatus (low rank apparatus) 30 from the recording device 210 of high-order apparatus 20 inside, and will transmit them to the encryption communication IC 205.
The data transmitted to the encryption communication IC 205 are transmitted to the information recording medium 211 via the recording-medium interface 207 as it is (writing).
[0189] If recording-medium attestation is not settled when controlled-system apparatus (low rank apparatus) 30 transmits data to an information recording medium, the encryption communication IC 305 of controlled-system apparatus (low rank apparatus) 30 starts attestation of an information recording medium.
If an information recording medium can be attested, CPU301 of controlled-system apparatus (low rank apparatus) 30 will read data from memory 302 or a recording device 309, and will transmit them to the encryption communication IC 305.
The encryption communication IC 305 enciphers the transmitted data with a session key, and transmits them to the information recording medium 310 by recording-medium interface 306 course.
[0190] Moreover, describe the case where data are exchanged between a service center 10 and high-order apparatus 20, during service offer.
The case where the data for service offer are transmitted from a service center 10 is described.
Data are first sent to the encryption communication IC 104 from the data base 103 for service offer by control of CPU101 of a service center 10.
The encryption communication IC 104 transmits to an external network via the external network interface 105, after enciphering with the session key exchanged between a service center 10 and controlled-system apparatus (low rank apparatus) 30 on the occasion of apparatus attestation of the data.
[0191] In the high-order apparatus 20 side, the encryption communication IC 205 receives data by external network interface 208 course, and transmits to the recording devices 210, such as memory 202 and a disk, through a data bus.

[0192] Describe the case where data are continuously transmitted to a service center 10 from high-order apparatus 20.
First, the data enciphered with the session key exchanged by control of CPU201 of high-order apparatus 20 between controlled-system apparatus (low rank apparatus) 30 and a service center 10 are read from memory 202 or a recording device 210, and are sent to the encryption communication IC 205.
The encryption communication IC 205 transmits the data to an external network via the external network interface 206.
In the service center 10 side, the encryption communication IC 104 decodes the data received by the external network interface 105 course using a session key.
The decoded data are transmitted to memory 102, the data base 103 for service offer, the apparatus information data base 106, and the user information data base 107 through a data bus.
While offering service, if required, CPU101 of a service center 10 will record fee collection information on memory 102 or the user information data base 107.
Fee collection information is the number of times of use of onerous service, time, the amount of transceiver data, etc.
[0193] As mentioned above, it is enciphered using a session key and the communication of data performed between a service center and apparatus during offer of service can protect the contents of communication.
If offer of service is completed, CPU101 of a service center 10 will acquire a user's settlement-of-accounts information from the user data base 107 by using User ID as a search key, and will perform settlement-of-accounts processing.
End processing is performed in case offer of service is ended.
[0194] In addition, when controlled-system apparatus (low rank apparatus) 30 is not equipped with an encryption function, after it does not encipher data but high-order apparatus 20 enciphers with a session key, data transmission is performed to a service center 10 between low rank apparatus and high-order apparatus.
After high-order apparatus 20 decodes the data from a service center 10 with a session key, they are transmitted to controlled-system apparatus (low rank apparatus) 30 through an information recording medium.
The protocol in this case is shown in Fig. 56.
[0195] Below [the example of concrete processing] explains the concrete example of service offer of the service offer system through the means of communication of this invention, and the service offer method.
[— 0196] <remote maintenance> — telediagnosis and a restoration system are first described as a concrete example of service offer.
The protocol in this case is shown in Fig. 57.
This system is an example which performs diagnosis and restoration of an obstacle part by operation from a service center 10, when an obstacle occurs to apparatus.

[0197] Diagnose in order to investigate the state of apparatus first.
This diagnosis is performed, when CPU (it is [in the case of high-order apparatus] CPU301 in the case of CPU201 and low rank apparatus) of apparatus publishes a command to various portions inside apparatus and analyzes that response.
The program for diagnosis is beforehand recorded on memory, a disk, etc. inside apparatus.
If diagnosis is completed, the result will be transmitted to a service center 10.
Or it is good also as composition which diagnoses by borrowing the help of a center.
In this case, apparatus transmits the message of a diagnostic request to a service center 10.
If diagnosis of applicable apparatus is possible for the service center 10 which received the message of a diagnostic request, it will publish a diagnostic command and will transmit it to apparatus.
If a diagnostic command is received from a service center 10, apparatus will execute the command and will transmit a result to a service center 10.
[0198] A service center 10 analyzes the result transmitted from apparatus, by it, if required, will publish a diagnostic command again and will transmit it to apparatus.
An analytic procedure is repeated from issue of the above-mentioned diagnostic command until a service center 10 can judge that diagnosis was completed.
Telediagnosis is performed as mentioned above and an obstacle part and a state can be specified, and if remote restoration is possible, it will go into the procedure of restoration.
Remote restoration is performed by transmitting a restoration command required in order that a service center 10 may restore the obstacle of apparatus to apparatus based on a diagnostic result.
[0199] CPU101 of a service center 10 analyzes a diagnostic result, and publishes a restoration command.
Under the present circumstances, the optimal command is chosen with reference to the obstacle history of the past of the applicable apparatus accumulated in the data base 103 for service offer, or this model.
A service center 10 transmits this restoration command to apparatus.
Apparatus executes the restoration command which received by control of CPU in apparatus, and transmits the result to a center.
The service center which received the result analyzes based on the result and past history, if required, will publish a restoration command again and will transmit it to apparatus.
The message to a user is displayed on the display section of apparatus if needed.
And it asks for the input of continuing execution of restoration.
An analytic procedure is repeated from issue of the above-mentioned restoration command until a center judges that restoration was completed or a user ends restoration.

In case restoration is ended, the diagnostic result till then and the contents of restoration are registered into the apparatus information data base 106.
It uses for fee collection, or the data of two or more apparatus are collectively fed back to an apparatus maker, and the diagnostic result and the contents of restoration which were registered into the data base can be used for the improvement of apparatus.
And a center notifies the end of remote restoration to apparatus.
[0200] Backup and restoration processing of the data saved to apparatus are explained as another example of service offer of <backup restoration> book invention about the processing composition which a service center 10 performs.
[0201] This is for using the apparatus with a former state by restoring, even if it should back up beforehand data, such as setting information saved to apparatus, for the memory means of a service center 10 and data should disappear.
Backup is explained first.
The protocol in this case is shown in Fig. 58.
[0202] Apparatus performs a backup start demand to a service center 10.
The service center 10 which received this demand secures the domain for backup on the data base 103 for service offer.
If it is in the state where partitioning is successful and it can back up, a service center 10 will transmit backup start confirmative advice to apparatus.
The apparatus which received start confirmative advice transmits the data for backup to a service center 10.
A service center 10 is saved to the domain which secured the received backup data.
An end of preservation registers backup information, such as backup time and a preservation domain, into the apparatus information data base 106.
And a service center 10 notifies the end of backup to apparatus.
[0203] Explain the procedure of restoration continuously.
The protocol in this case is shown in Fig. 59.
Apparatus performs a restoration start demand to a service center 10.
The service center 10 which received this demand acquires backup information from the apparatus information data base 106 by using Apparatus ID as a search key.
If it is in the state where it succeeds in acquisition of backup information, and can restore, a service center 10 will transmit restoration start confirmative advice to apparatus.
And a service center 10 takes out the domain information on the data base 103 for service offer with which backup data are saved from backup information.
Based on this information, backup data are read from the domain on the data base 103 for service offer, and it transmits to apparatus.
[0204] Apparatus performs restoration, after checking the received backup data.
After restoration is completed, apparatus notifies the end of restoration to a service center 10.

The service center 10 which received the notice of a restoration end registers a restoration history into the apparatus information data base 106.
And a service center 10 notifies the end of the processing about restoration to apparatus.
[0205] Data distribution is described as still more nearly another example of service offer of <data distribution (music, image, text, etc.)> book invention.
[0206] This stores data, such as music, and an image, text, in a service center 10, and can take in and use them for apparatus from a service center 10 according to a demand of a user.
The protocol in this case is shown in Fig. 60.
In using a data distribution function, a user first performs operation which starts data distribution by the control unit (it is [in the case of high-order apparatus] a control unit 308 in the case of a control unit 209 and low rank apparatus) prepared in apparatus.
The apparatus which received the input from a user performs a data distribution start demand to a service center 10.
If a service center 10 is in the state where data distribution can be performed, it will transmit data distribution start confirmative advice to apparatus.
The apparatus which received start confirmative advice displays the message of a data distribution start on the display section (in the case of high-order apparatus, in the case of the display section 203 and low rank apparatus, it is the display section 303).
Furthermore, a service center 10 transmits the menu containing the choice about the data which can be used to apparatus.
Apparatus will be outputted to the display section, if this menu is received.
[0207] If a user chooses required data out of a menu and inputs into a control unit, the information, for example, a data number, what selected data of apparatus are will be transmitted to a service center 10.
A service center 10 acquires required data from the data base for service offer, and transmits them to apparatus.
Apparatus outputs having received data to the display section.
And a user operates reproducing data etc.
What is necessary is just to perform a required input from a control unit, when a user uses a data distribution function succeedingly.
After data distribution is completed, if the service center 10 is required, a data distribution history will be registered into the apparatus information data base 106.
It uses for fee collection or the data distribution history registered into the data base can be used for marketing, such as examination of the data offered after gathering the data of two or more apparatus.
And a service center 10 notifies the end of data distribution to apparatus.
[— 0208] <help tutorial> — the example which offers further the help function which explains the operation method of apparatus as another example of service offer of this invention is described.

This stores the help data which explain the operation method of apparatus in a service center 10, takes a required portion into apparatus according to a demand of a user, and shows it to a user.
The protocol in this case is shown in Fig. 61.
[0209] although it is also possible to save all help data to apparatus about this help function, there are all that there may be few domains for preservation or holding always new help data in apparatus from a difficult thing — it is — it is the example made into the form which puts some help data on a service center 10.
In using a help function, a user first performs operation which starts a help by a control unit (it is [in the case of high-order apparatus] a control unit 308 in the case of a control unit 209 and low rank apparatus).
The apparatus which received the input from a user performs a help start demand to a service center 10.
If it is in the state where help data can be offered, a service center 10 will transmit help start confirmative advice to apparatus.
[0210] The apparatus which received start confirmative advice transmits the data which specify the required portion of a help to a service center 10.
The service center 10 which received this acquires required help data from the data base 103 for service offer, and transmits them to apparatus.
Apparatus displays the received help data on the display section (in the case of high-order apparatus, in the case of the display section 203 and low rank apparatus, it is the display section 303).
What is necessary is just to perform a required input from a control unit, when a user uses a help function succeedingly.
An end of offer of help data registers a help offer history into an apparatus information data base.
And a center notifies the end of a help to apparatus.
[0211] Moreover, it is possible not only a simple help but to offer a tutorial, namely, to consider it as the composition which offers operation information.
This is a function for a user to master the usage of apparatus, and if each portion of apparatus is operated, a display and an operation form will change according to the situation.
The protocol in this case is shown in Fig. 62.
In using a tutorial function, a user performs first operation which starts a tutorial by a control unit.
The apparatus which received the input from a user performs a tutorial start demand to a center.
If it is in the state where a tutorial can be performed, a center will transmit tutorial start confirmative advice to apparatus.

The apparatus which received start confirmative advice displays the message of a tutorial start on the display section.
If a user operates apparatus, apparatus will transmit the contents of operation, and the internal state of apparatus to a service center 10.
A service center 10 determines the data with which the next should be provided based on these information.
And required tutorial data are acquired from the data base for service offer, and it transmits to apparatus.
[0212] Apparatus displays the received tutorial data on the display section.
What is necessary is just to perform a required input from a control unit, when a user uses a tutorial function succeedingly.
An end of offer of tutorial data registers a tutorial offer history into an apparatus information data base.
And a center notifies the end of a tutorial to apparatus.
[0213] It has explained in detail about this invention, referring to a specific case of the operation above.
However, it is obvious that this contractor can accomplish correction and substitution of this case of the operation in the range which does not deviate from the summary of this invention.
That is, with the form of illustration, this invention has been indicated and it should not be interpreted restrictively.
In order to judge the summary of this invention, you should 酌 the column of the claim indicated at the beginning 3 times.
[0214] As beyond the [effect of invention] has explained, according to the service offer system through the means of communication of this invention, the service offer method, service agency equipment, and the program offer medium
It becomes possible to receive the information from a service center from the high-order apparatus which has a means of communication through a local network or an information recording medium, even when apparatus is a service center and the composition which does not make direct connection.
It is not necessary for all the required controlled-system apparatus (low rank apparatus), such as control and a maintenance, to constitute the means of communication of the communication interface for connecting with an external network etc.
[0215] According to the service offer system through the means of communication of this invention, the service offer method, service agency equipment, and the program offer medium, further
Even if it is the composition that required controlled-system apparatus (low rank apparatus), such as control and a maintenance, is not equipped with an encryption function

In order to perform communications processing with a service center after the high-order apparatus which can communicate enciphers data through controlled-system apparatus (low rank apparatus), a local network, or an information recording medium,
Even if it goes via the public network where the safety of communication data is not guaranteed, prevention of disclosure of important information, such as personal information which is needed in order to offer control information or control information, is attained.